Title: The Information Systems Department ("BIDMC-IS") Data Security Policy

Policy #: ADM-04

Purpose: Beth Israel Deaconess Medical Center ("BIDMC") is committed to ensuring the confidentiality, integrity and availability of its Protected Data by implementing a comprehensive Information technology ("IT") security management program. The program includes administrative, technical and physical safeguards appropriate to the size and complexity of the organization.

The safeguards identified in this policy are the minimum controls necessary to ensure appropriate protection for BIDMC's Information Systems and Protected Data. Where more robust safeguards are reasonable and appropriate, they shall be implemented.

Scope: The IT security management program's scope includes electronic data in use, in transit or at rest. It includes audio data that is stored in an electronic form as well as facsimile transmissions where the data is in an electronic form before it is transmitted. The program scope does not include data in paper form.

Definitions: The definitions and acronyms for terms used in this policy are included at the end of this document.

Section Index

Policy Statement

Security Management Process

A. Overview

1. Scope – Except as otherwise noted in this policy, the IT security process covers all persons and things that access, transmit, or store electronic data on BIDMC's Information Systems. BIDMC-IS considers the following in the selection, implementation, and on-going support of security controls:
    a. BIDMC's size, complexity and capabilities;
    b. BIDMC's technical infrastructure, hardware and software security capabilities;
    c. The costs, including operational impact;
    d. The probability and potential impact of security risks; and
    e. The need for defense-in-depth.
2. Components – The IT security program includes:
    a. A comprehensive risk analysis and mitigation plan;
    b. Buffers, barriers and monitors to detect and contain security violations;
    c. An auditing program for tracing security violations to their source;
    d. Transmission security management;
    e. User security management;
    f. An incident response, disaster prevention and recovery plan;
    g. An acceptable use policy; and
    h. A workforce training and education program focused on IT security.
3. Assignment of Responsibility - The Chief Information Officer (CIO) is responsible for ensuring that BIDMC appropriately protects the confidentiality, integrity and availability of IT resources, especially

those containing Protected Data. The CIO has named the Chief Information Security Officer (CISO) as his designee for the purposes of this policy.

The above notwithstanding, information security is a responsibility shared by senior BIDMC leaders, BIDMC managers and Workforce Members, business and system owners, BIDMC-IS professionals, and all other Users of BIDMC Protected Data and Information Systems. Nothing in this policy voids the responsibility of these BIDMC stakeholders for securing Protected Data.

4. Policy Enforcement – The CIO or his/her designee works with other management officials, as appropriate, to bring about corrective action when violations of IT security-related policies are detected.

B. Risk Analysis & Mitigation

1. Risk Analysis Process – At least annually, the CIO or his/her designee will coordinate an update to the risk analysis for systems managed by BIDMC-IS. The risk analysis will identify security dangers, relative risk, probable impact, and security measures needed to make systems less vulnerable. The CIO or his/her designee will coordinate interim updates to the risk analysis and risk mitigation plans when warranted by new security threats, major changes to BIDMC's Information Systems and lessons learned from recent security incidents.
2. Categorization of Information and System Assets –In coordinating the risk analysis process, the CIO or his/her designee gives priority to applications containing highly sensitive, personally identifiable data whose compromise could lead to highly damaging publicity, clinical harm, major fraud, wide-scale identity theft, or business disruption. The CIO or his/her designee may group systems by technology, location, job code, or other meaningful category to improve the efficiency of the process. For each asset category, the CIO or his/her designee should complete the following tasks as part of the risk analysis:
    a. Identify major threats to confidentiality, availability, or data integrity;
    b. Assign a risk category based on the likelihood of occurrence and probable impact of an incident;
    c. Request the active participation of system, data and business owners; and
    d. Identify security measures needed to reduce the threat or lessen the impact to reasonable and appropriate levels.
3. Inventory of Assets – The risk analysis includes a perpetual inventory of operationally significant IT systems and processes.
4. Security Screening – Prior to introducing a new IT system or a material change to an existing system, the CIO or his/her designee screens the system to determine if it presents a material risk to BIDMC. The depth of screening depends on factors such as the sensitivity of the data, number of Users, Internet exposure, and known vulnerabilities. The CIO or his/her designee determines the process for conducting the security screenings. Where the CIO or his/her designee determines that a system or change presents a material risk, the system will be withheld from production until the risk is satisfactorily mitigated.

System Protections

C. Buffers, Barriers and Monitors

1. The CIO or his/her designee coordinates the use of technologies and processes that record, examine, and, as appropriate, filter or block activities that present security threats to BIDMC's Information Systems and Protected Data.
2. The CIO or his/her designee must ensure that the monitoring activities include:
    a. Intranet and Extranet activities insofar as they introduce risk to BIDMC's Information Systems;
    b. Timely review, analysis and reporting of system logs; and
    c. Log preservation to facilitate after-the-fact investigations of security incidents in collaboration with the Department of Public Safety, Office of Business Conduct, Office of General Counsel and/or Human Resources Department, as appropriate.
3. BIDMC-IS must select system monitoring activity targets based on the risk analysis, paying particular attention to critical, high impact systems and those with the greatest security incident-related activity.

D. Information System Audits

1. The CIO or his/her designee coordinates IT auditing activities with other BIDMC organizations involved in similar work, i.e. the Department of Public Safety, Office of Business Conduct, Office of General Counsel, Internal Audit and Human Resources Employee Relations.
2. BIDMC Workforce Member must not use their access to IT systems to monitor the activities of another person without that person's knowledge unless the monitoring activity is:
    a. A legitimate part of their job function; or
    b. Part of an investigation authorized by the Department of Public Safety or other law enforcement authorities, the Office of General Counsel, the Office of Business Conduct or the Human Resources Department.
3. To the extent practical, the CIO or his/her designee should ensure that IT system audit logs contain sufficient information to establish the following:
    a. The type of event that occurred;
    b. When the event occurred (date, time);
    c. Where it occurred;
    d. The source of the event;
    e. The outcome of the event; and
    f. The identity of any User, application or Workstation associated with the event.
4. BIDMC-IS protects audit information and audit tools from unauthorized access, modification or deletion.

E. Results of Audit and System Monitoring Activity

1. The CIO or his/her designee uses the observations and investigative results generated from the above programs to improve the quality of:
    a. The IT security management process; and
    b. The training and awareness programs for Workforce Members.

User Security and Access Controls

F. Securing BIDMC's Information System

1. The CIO or his/her designee ensures that there is a formal process for granting access to Protected Data that includes:
    a. Documentation of the business need and the responsibilities of both the grantee and the Management Sponsor; and
    b. A requirement that each application for access to an IT system with Protected Data is evaluated and approved by a Management Sponsor.
2. When appropriate, different types of accounts or group rights may be used to customize access levels. These may include but are not limited to Users, Service Accounts, Vendors, Contractors, Consultants, System Administrator, Training, Testing, and/or Research Collaborator.
3. Prior to gaining access to Protected Data:
    a. Workforce Members must complete all necessary training requirements and execute appropriate access agreements that may include, but are not limited to non-disclosure agreements, acceptable use agreements, conflict of interest agreements and acknowledgements that the User has read and understood BIDMC policies and procedures; and
    b. Management Sponsors must ensure that Users who are not Workforce Members have a valid Business Associates Agreement in place that complies with the requirements of BIDMC Policy # PV-17 (Business Associates and Business Associate Agreements with the BIDMC Organized Health Care Arrangement) or such other documentation as is required by BIDMC policies or applicable regulations.

G. Maintaining Appropriate Access

1. Management Sponsors must re-evaluate the appropriateness of Users' access as part of a Workforce Member's annual evaluation, where applicable, as well as whenever:
    a. The User's job or contractual responsibilities change; or
    b. The User transfers to a new position; or
    c. Upon the renewal or expiration or a third party contract that requires access to BIDMC's Information Systems or Protected Data.
2. Management Sponsors promptly notify the BIDMC-IS' Call Center ("Help Desk") when access privileges for a User that they sponsored need to be downgraded or terminated. BIDMC-IS promptly terminates or changes access once notification is received.
3. Where the termination is involuntary, managers must evaluate the risk associated with the termination and, when appropriate, request that BIDMC-IS terminate access privileges no later than the time at which the User is terminated.
4. Following or, where feasible, in anticipation of a termination, managers must ensure that all Protected Data in the possession of the User is retrieved and that any security passwords or encryption keys are provided to appropriate BIDMC staff prior to the User's departure from the premises.

H. User Authentication

1. Administrators of BIDMC-administered Information Systems implement a process for authenticating Users that incorporates the following elements:
    a. Assignment of a unique user ID that is not later re-used for another User;
    b. Where technically feasible, implementation of centralized control of user IDs and other Information System identifiers;
    c. Implementation of a secure mechanism for assigning and resetting passwords that includes, but is not limited to a requirement that Users reset their initial password;
    d. Controlled access and secure transmission of authentication data to prevent Users, including system administrators, from gaining unauthorized access to the data. Where appropriate based on a risk analysis, encryption will be used;
    e. Enforcement of strong passwords, where the strength for a particular User, or class of Users, may vary based on the risk associated with the User or User class;
    f. With the exception of vendor, system support and resource accounts, disabling of accounts after 90 days of inactivity;
    g. For Web-based applications, termination of a User's authenticated session after no more than 20 minutes of inactivity; and
    h. Temporarily blocking access to a User account following six (6) unsuccessful login attempts.

Acceptable Use

I. BIDMC Information System & Data Assets

1. BIDMC Ownership – BIDMC is the sole and exclusive owner of any and all components of its Information System, including but not limited to:
    a. Computer Information or other data that is created, received, maintained or transmitted by BIDMC, regardless of the ownership of the device or media on which it is stored; and
    b. E-mail addresses assigned by BIDMC.
2. System Administration – If a device is not under central BIDMC-IS management, the department or person responsible for the device must assign an appropriately skilled administrator to manage the system.
3. Sharing BIDMC Information System Resources – Users must not:
    a. Install any software that allows the BIDMC Information System or any of its components to be shared as resources to the Internet (e.g. some peer-to-peer software allows your system to be accessed by non-BIDMC systems); or
    b. Copy or distribute any BIDMC-licensed software for personal use or the use of a third party

without prior authorization of the CIO or his/her designee.

4. Users have no expectation of privacy – Users understand and agree that they have no expectation of personal privacy of any kind related to their use of the BIDMC's Information System, irrespective of the User's application of passwords to protect their personal or business data or their efforts to delete such data from the Information System.

    a. BIDMC retains the right, with or without cause or notice to the User, to:

        i. Access any data stored on its Information System regardless of ownership, including but not limited to e-mail messages; and

        ii. Monitor User activities, including but not limited to their use of the Internet.

    b. To the extent that any right to privacy or similar right remains, Users expressly waive those rights with respect to their use of any component of BIDMC's Information System or any data stored thereon.

J. Access to the BIDMC Information System

1. Minimum Necessary access –BIDMC provides Users with access to its Information System to enable Users to carry out their job responsibilities.

    a. Users must not use BIDMC's Information System to access the records of patients or employees unless the User is accessing the records as a legitimate part of their job function.

    b. Users must not access, read, copy or modify private files, e-mail messages or data that is created by or intended for another person, including but not limited to those whom the User supervises, without the prior consent of that person or written authorization from authorized BIDMC personnel (e.g. Office of the General Counsel, Office of Business Conduct or Human Resources Employee Relations).

2. Compliance with laws and policies – In the course of using BIDMC's Information System, Users must comply with all software licenses, copyrights, and all other state, federal and international laws, in addition to all BIDMC policies and related documentation. BIDMC reserves the right to revoke access for any User who violates these laws or BIDMC's policies.

3. Passwords Protection – Users are prohibited from sharing their password with others or accessing BIDMC's Information System using another User's user ID and password. Users must take reasonable steps to safeguard their password from being disclosed to others. BIDMC holds Users responsible for transactions made by others using their user ID and password if there was intentional sharing or blatant disregard for basic security precautions.

4. No additional rights – This Policy is not intended and does not grant to Users any contractual rights.

K. Use of BIDMC's Information System Resources

1. Appropriate use – Users must use BIDMC's Information System responsibly and in a professional, ethical, and lawful manner.

2. Personal use – Users may use BIDMC's Information System resources for limited and appropriate personal purposes, provided that their personal use does not:

    a. Interfere with the User's work performance or that of any other User;

    b. Impair the performance of the Information System;

    c. Conflict with technical safeguards that have been implemented;

    d. Result in any material expense to BIDMC; or

    e. Violate any provision of this or any other BIDMC policy or related document, including, but not limited to BIDMC's Code of Conduct.

3. Prohibited activities – Users must not use BIDMC's Information System for any of the following activities:

    a. Revenue-producing activities that are for the benefit of the User or a third party (including but not limited to the sale of any non-BIDMC products or services);

    b. Soliciting others for political reasons, special interests, philanthropy or other causes unrelated to BIDMC's business;

c. Engaging in the unauthorized sharing or copying of digital audio music files, software, photographs or any other copyrighted material, using peer-to-peer networks or by any other means;

d. Creating, transmitting, copying, displaying or storing Inappropriate or Unlawful Content except as part of an active investigation sanctioned by the CIO or his/her designee and conducted in collaboration with the Office of Business Conduct, Office of General Counsel or the Human Resources Department, as appropriate;

e. Altering, bypassing or otherwise circumventing or disabling any of the safeguards identified in this policy; or

f. Accessing the Internet using a Workstation and modem, except where the use of a modem is for business purposes and the use of an alternative mechanism is operationally infeasible.

4. BIDMC's e-mail system – Users must use e-mail responsibly and professionally. Users must not do any of the following:

a. Send Inappropriate or Unlawful Content by e-mail or some other form of electronic communications using BIDMC's Information System, e.g. bulletin board systems, newsgroups, chat groups, Twitter, Facebook, MySpace, Blogs, or other forms of social networking;

b. Send anonymous or pseudonymous electronic communications;

c. Distribute e-mail messages that consume a disproportionate amount of transmission or storage resources;

d. Alter the "From" line or other e-mail content or online posting to attribute the authorship to the wrong party;

e. Auto or manually forward messages from their BIDMC e-mail account to a third party system without prior approval by the CIO or his/her designee;

f. Use personal, non-BIDMC e-mail accounts to send Protected Data;

g. Address or forward e-mail containing Protected Data without exercising caution to ensure that it does not go to the wrong party and that the distribution is limited to only those with a need-to-know; and

h. Forward content tagged as "Confidential" or "Attorney-Client Privileged" unless authorized by the sender.

L. Transmitting and Sharing BIDMC Protected and Other Data

1. Transmission Security Strategy - BIDMC-IS develops and implements a strategy for securing the confidentiality, integrity and availability of BIDMC's Protected Data as it is transmitted across both internal and external electronic communication networks. The strategy mitigates risks to data-in-transit to reasonable and appropriate levels while continuing to meet BIDMC's operational business needs.

2. Sharing BIDMC Protected Data – Users are permitted to use the Internet and BIDMC Intranet to assist them in the performance of their jobs. Users must not disclose or discuss BIDMC Protected Data or BIDMC Confidential or Proprietary Information in online forums, including but not limited to bulletin board systems, newsgroups, chat groups, Facebook, Twitter, MySpace or Blogs.

3. Transmission of Protected Data – Users must not transmit or electronically exchange any of BIDMC's Protected Data through e-mail or any other transmission mechanism that is not a BIDMC-approved, encrypted telecommunication channel. Where applicable, the transmission of Protected Data must also be in accordance with a valid Business Associates agreement or other data sharing agreement.

M. Ensuring the Integrity of BIDMC's Information System

1. User Precautions – Users must take reasonable precautions to ensure that they do not introduce a virus, spy ware or other malicious software into the BIDMC Information System environment. In particular, the following practices are prohibited:

a. Intentionally creating, storing, or distributing malicious software (e.g., viruses, worms, or other destructive code);

b. Installing software or hardware that increases BIDMC's vulnerability to security threats;

c. Accessing external computer services that increase BIDMC's vulnerability to denial of service

attacks, viruses, or similar problems (e.g. peer-to-peer services);

d. Opening suspicious e-mail attachments received, especially from unknown sources;

e. Accessing the network with a diagnostic or testing tool, such as a protocol analyzer intended to monitor, decode, or filter packets of information unless such access is a legitimate part of your job function; and

f. Using a modem to access BIDMC's network unless you have prior approval from the CIO or his/her designee.

N. Storage of Protected Data

1. Local Storage of Protected Data – All Protected Data should be saved to servers or storage devices housed in one of the data centers managed by BIDMC-IS. Users should not save copies of Protected Data on their local devices except where the device is a Mobile Device that meets the requirements of this policy.

2. Storage on External Systems – Users must not employ software that copies BIDMC's Protected Data to an external system unless BIDMC has a valid Business Associates or confidentiality agreement, as applicable, with the company hosting the external system. External systems include but are not limited to Google Documents and other personal Internet-based storage services.

3. Hosted Data Services – Prior to contracting with an external organization to host an application containing BIDMC's Protected Data, the CIO or his/her designee must perform a security review and approve the external hosting arrangement.

O. Duty to Report

1. Activities to Report – Users must immediately report any instance or suspected instance of the following activities to the identified authority:

    a. Report suspected computer viruses or other suspicious activity on BIDMC-administered Workstations or laptop computers to the Help Desk;

    b. Report to the Office of Business Conduct any unauthorized sharing of BIDMC's Information System resources;

    c. Report to the Office of Business Conduct any instances of an actual or possible Data Breach involving Protected Data, including but not limited to:

        i. Transmission of unencrypted Protected Data across the public Internet;

        ii. Transmission of Protected Data to an unauthorized recipient; or

        iii. The receipt, in error, of Protected Data by any mechanism;

    d. Report to the Department of Public Safety, Office of Business Conduct, and Help Desk the loss or theft of a Workstation, Mobile Device or Electronic Media, regardless of ownership; and

    e. Report to the Department of Public Safety and the Office of Business Conduct the loss or theft of any device (such as an access card or physical key) that provides physical access to areas where components of the Information System are housed.

P. Protecting the BIDMC Data Network

1. Except where the User is an authorized member of the IT Workforce who is carrying out authorized job functions, Users must not take any of the following actions without the express permission of the CIO or his/her designee:

    a. Connect a device to the data network, other than the wireless guest network, without prior coordination and approval of BIDMC-IS;

    b. Install, modify or remove a wireless access point;

    c. Enter a designated data network or telecommunications equipment room without written authorization from BIDMC-IS; and

    d. Attempt to physically or logically reconfigure, move, or disengage a data network component.

Workstation Security

Q. Risk-Based Approach

1. For each class of Workstations used by BIDMC Users, BIDMC-IS implements safeguards responsive to the threats and vulnerabilities identified in BIDMC's risk analysis. The combination of safeguards applied to a particular class of Workstations must be documented and appropriately balance the needs of the Users with BIDMC's commitment to mitigating its risk to reasonable and appropriate levels.

R. Securing the Physical Surroundings

1. BIDMC must implement the following safeguards, where appropriate for a particular class of Workstations:
    a. Workstations are located in areas that minimize the risk of harm from physical and environmental hazards;
    b. Workstations, printers and displays are physically located in such a manner as to minimize the risk that unauthorized persons will gain access to them; and
    c. Display screens are positioned or configured with privacy screens such that information cannot be viewed through a window, by persons walking in a hallway, or by persons waiting in the reception or other public areas.
2. Users must ensure that laptop computers used for BIDMC's business are secured with a laptop lock or some other equivalent physical measure when left unattended, both inside and outside of the BIDMC facilities.

S. Enforcing Access and Other Controls

1. System administrators configure Workstations to comply with the requirements of this policy. These requirements include but are not limited to:
    a. Requiring Users to have a username and password to access the Workstation;
    b. Masking or otherwise obscuring passwords when entered; and
    c. Enabling a screensaver with no more than a 10-minute timeout period and locking the User session after the same period of inactivity.
2. In accordance with industry best practices and as technically and operationally feasible, system administrators implement the following controls for BIDMC-administered Workstations:
    a. Limit User access to local administrative privileges; and
    b. Restrict Users ability to install any software without first consulting the Help Desk.

T. Implementing Technical Safeguards

1. Where technically feasible, system administrators must ensure that BIDMC-administered Workstations that connect to the BIDMC network have the following safeguards in place:
    a. Operating system and application security patches must be up-to-date and kept current;
    b. IS-sanctioned anti-virus software must be activated and updated daily via BIDMC's network or another source approved by BIDMC-IS. Copies of appropriate software may be obtained from the Help Desk for use on BIDMC-administered Workstations and laptop computers;
    c. Workstations must comply with BIDMC's Standard Naming Convention to ensure the Workstation can be easily identified on the BIDMC network;
    d. Each Workstation must join the Active Directory domain and have the necessary technology installed to enable BIDMC to effectively and efficiently manage its Information System resources; and
    e. BIDMC-IS must retain local administrator rights on the Workstation.
2. Where the above listed safeguards are not feasible, the system administrator must put mitigating controls in place to reduce the risk to reasonable and appropriate levels.

U. Obligations of Users

1. Users must not attempt to gain unauthorized access to any component of BIDMC's Information

Systems.

2. Users must logout or lock their Workstation before leaving it unattended. Where locking or logging out of their Workstation is not technically or operationally feasible, the User must logout of any application that provides access to Protected Data.
3. Users who manage BIDMC-administered Workstations must ensure that:
    a. They obtain prior approval from BIDMC-IS prior to implementing encryption software on BIDMC-administered Workstations; and
    b. A BIDMC supervisor has the current encryption password or keys for any encryption solution used.

Mobile Device Security

V. User Obligation to Secure Mobile Devices

1. Where technically feasible, Users will apply the following safeguards for Mobile Devices that connect to the BIDMC network and/or are used to access, store, transmit or process Protected Data:
    a. Password protection;
    b. Timeout periods that require re-entry of the password;
    c. No more than 10 password attempts before the device content is wiped;
    d. Regularly updating anti-virus and other security software;
    e. Encrypting Protected Data;
    f. Disabling unnecessary services, wireless interfaces and applications (e.g. BlueTooth) when not needed; and
    g. Installing a device firewall.
2. Users must:
    a. Keep their Mobile Device in their possession, especially when traveling or in an uncontrolled environment (e.g., in a hotel room, a vendor's facility, or remote location) or, if necessary, secure the device through some other means;
    b. Prevent unauthorized persons from accessing BIDMC's files stored on the device, or using the device to gain access to BIDMC's network;
    c. Report immediately the loss or theft of a Mobile Device owned by BIDMC or suspected to contain BIDMC's Protected Data; and
    d. Dispose of any Mobile Device containing BIDMC Protected Data in accordance with this policy.

W. Laptop Computer Compliance

1. In the event there is a conflict between the Workstation and Mobile Device Security provisions, the provision that provides the greatest security to the data and the device must be applied.

Media Controls

X. Joint Obligation to Secure Media

1. BIDMC must:
    a. Protect and manage Protected Data throughout the lifecycle of any Electronic Storage Media that contains it; and
    b. Restrict access to Electronic Media that stores or transmits Protected Data in accordance with BIDMC's facility access controls and the requirements of this policy.
2. Users who store BIDMC's Protected Data on removable Electronic Storage Media ("Removable Media") must establish procedures to track and control such media, regardless of whether the data stored on the device is current or obsolete.
3. "Removable Media" includes but is not limited to floppy disks, zip disks, CD's, USB drives and memory sticks, regardless of ownership, as well as any Mobile Devices that are not administered by BIDMC, but on which BIDMC Protected Data is stored.

Y. Joint Obligation for Proper Re-Use or Disposal

1. Prior to disposal or reuse elsewhere, the person or department responsible for Electronic Storage Media must ensure that the media is cleared, purged, or destroyed in such a manner that any Protected Data cannot be read or reconstructed.
2. BIDMC may use an industrial data destruction service or facility but it must ensure that the Business Associate Agreement or services contract includes an obligation to comply with the appropriate state and federal media disposal requirements and a mechanism to verify that proper disposal has taken place.
3. Users who have Electronic Storage Media that is not administered by BIDMC but on which BIDMC's Protected Data is stored must ensure that the media is disposed of in accordance with this policy.

Z. User Obligations

1. Users are obligated to control, track, re-use and dispose of media in accordance with this policy, including but not limited to sections X and Y.
2. Terminations - Upon termination of their relationship with BIDMC, Users must immediately and in any event prior to leaving BIDMC's premises:
    a. Dispose of any Electronic Storage Media that contains BIDMC's Protected Data in accordance with this policy; or
    b. Ensure that BIDMC's Protected Data is removed from the Electronic Storage Media prior to re-use, in accordance with this policy; or
    c. Present the Electronic Storage Media to their supervisor, contracting department or BIDMC-IS for disposal or re-use, in BIDMC's sole discretion.
3. Transfer of BIDMC-Administered Media with a Research Grant - Where BIDMC-administered Electronic Storage Media is moving with a BIDMC research grant to another institution, the User or department responsible for that media must:
    a. Notify CIO or his/her designee of the pending transfer of the media to another institution;
    b. Provide documentation to the CIO or his/her designee that demonstrates that the media was purchased with monies from the research grant;
    c. Where the media does not contain BIDMC Protected Data, provide a signed acknowledgement to the CIO or his/her designee stating that fact;
    d. Where the Electronic Storage Media does contain BIDMC's Protected Data, provide to the CIO or his/her designee:
        i. Appropriate documentation that demonstrates that the User is authorized to move the Protected Data to another facility; or
        ii. Before the media is transferred, documentation confirming that BIDMC's Protected Data has been removed in accordance with this policy; and
    e. Upon request, permit the CIO or his/her designee to inspect the Electronic Storage Media before it is removed from BIDMC's premises to verify that it does not contain BIDMC's Protected Data.

Remote Access Security

AA. Securing Remote Access

1. BIDMC-IS:
    a. Provides Users with a list of approved methods for remotely connecting to the BIDMC network;
    b. Grants remote access to Users based on business need and the results of its most current risk analysis;
    c. Ensures that transport security over approved remote access methods is appropriate for the content communicated and that the network connection is terminated at the end of a network session; and
    d. Monitors and disables remote access accounts showing suspicious activity. The accounts will

remain disabled until the CIO or his/her designee investigates and resolves the matter.

BB. User Obligations

1. Users who remotely connect with BIDMC's Information System are prohibited from connecting through methods not officially approved by BIDMC-IS (e.g. GotoMyPC).
2. Prior to remotely connecting to BIDMC's Information System, Users must:
    a. Ensure the device from which they are connecting has up-to-date patches and anti-virus software;
    b. Use only approved remote control software to connect to the BIDMC network; and
3. Once a User is remotely connected to BIDMC's Information System, the User must ensure that:
    a. The User does not leave the system unattended without first logging out; and
    b. People who lack proper BIDMC-IS credentials are not permitted to use the remote access for any purpose.

Incident Response

CC. Computer-Related Incident Response (CIR) Plan

1. The CIO or his/her designee coordinates the development, documentation, implementation, and on-going maintenance of the plan to quickly and effectively respond to Computer-Related Incidents. The plan goals include:
    a. Responding in a manner that achieves and balances the following priorities:
        i. Minimizing harm to Protected Data and Information Systems;
        ii. Ensuring the availability of data in support of the safe, effective, and timely delivery of patient care;
        iii. Investigating the cause(s) of the Computer-Related Incident; and
        iv. Promptly restoring normal IT services;
    b. Determining whether the confidentiality, integrity and availability of BIDMC's Information Systems have been compromised, particularly whether a Data Breach has or may have occurred;
    c. Collecting evidence in a manner that supports criminal, civil or disciplinary sanctions, as appropriate;
    d. Managing the information collected in a manner that ensures appropriate access; and
    e. Periodically testing the computer-related incident response plan, including each team's role in that plan.

DD. Computer-Related Incident Response Team (CIRT)

1. The Computer-Related Incident Response Team (CIRT) includes those BIDMC-IS Workforce Members who are required to effectively respond to any given Computer-Related Incident.
2. Where a Computer-Related Incident raises security issues or there is a known or suspected Data Breach, the CIRT must notify the CISO or his/her designee. The CISO's involvement with the CIRT may vary based on the nature of the Computer-Related Incident.

EE. Lessons Learned

1. As soon as possible, the CIO or his/her designee will hold a meeting to review the Computer-Related Incident. The meeting will include key CIRT team members, and, at the discretion of the CIO or his/her designee, additional BIDMC-IS Workforce Members whose input may be valuable to the post-incident analysis.
2. The Incident Review Meeting will review the effectiveness with which the incident was handled and recommendations for changes to security controls to prevent the incident from recurring.
3. The CIO or his/her designee will ensure that lessons learned are used to improve BIDMC-IS' processes and controls, particularly the computer-related incident response plan and risk analysis activities.

FF. Contingency Planning Process

1. The CIO or his/her designee is responsible for coordinating a plan for responding to events that risk catastrophic damage or failure to any Information System that contains Protected Data or on which BIDMC's critical business activity depends.

GG. Content of the Contingency Plans

1. The Contingency Plan:
    a. Includes comprehensive Disaster Recovery and data backup Plans that are consistent with BIDMC's business objectives and the results of the most recent risk analysis;
    b. Is designed to minimize the harm caused and ensure the timely resumption of the most critical Information Systems and processes; and
    c. Includes a list of triggering events that activate recovery operations, a plan for communications, a description of the roles and responsibilities of Workforce Members, provision for alternate operational site and key services, and a security plan to appropriately protect Protected Data during the recovery period.
2. Disaster Recovery and data backup plans should be developed for each critical Information System identified in the risk analysis categorization process. Recovery Time and Recovery Point Objectives will be consistent with the level of risk and the criticality of the Information System to BIDMC.
3. The CIO or his/her designee will ensure that:
    a. Contingency Plans are coordinated with BIDMC's Emergency Management Program, as applicable; and
    b. Distribution of Contingency Plans is controlled to protect potentially sensitive operational and personnel information.

HH. Contingency Plan Training and Testing

1. The CIO or his/her designee will coordinate periodic education and training activities to keep Workforce Members and Contingency Plan staff abreast of Contingency Plans, test their effectiveness, and incorporate ideas for improvement into future versions of the plans.
2. Quarterly exercises are held to test selective portions of the Contingency Plans.

II. Formal Data Backup Process

1. BIDMC-IS has a formal, documented backup plan for Information Systems. The plan:
    a. Identifies Protected Data, applications, and system and security documentation that will be backed up ("Backup Assets");
    b. Provides appropriate backup schedules that reflect the criticality and sensitivity of those Backup Assets, the risks associated with them and the frequency with which the data is modified;
    c. Identifies where backup media are stored, how it is secured and who has access to it; and
    d. Outlines procedures for restoring Backup Assets including the persons responsible for restoration.
2. BIDMC-IS develops Recovery Time and Recovery Point Objectives that are consistent with the application's priority and BIDMC's business requirements.
3. BIDMC-IS conducts, documents and periodically reviews monitoring and testing activities for both the backup and restoration phases. BIDMC-IS promptly resolves any problems to ensure that the program's ability to meet operational requirements is not at risk.

JJ. Securing Backup Assets

1. BIDMC-IS securely stores backed up data and associated documentation in a geographically diverse location from the primary data location.

Documentation

KK. IS Systems Documentation

1. System administrators document the applications they manage in a comprehensive manner and make that documentation available to other BIDMC-IS Workforce Members who have a need-to-know.
2. BIDMC-IS implements a process for periodically updating and publishing application documentation that ensures that all affected parties are aware of the must current version of the documentation and know how it can be accessed.
3. System administrators must publish documentation in an electronic format that permits affected parties to fully search the text of the document.

Exemption Request Process

LL. Request for Exemption

1. A BIDMC User or technology representative may request a temporary exemption from a BIDMC-IS policy where they are able to demonstrate that the approved IT process does not meet a business need and the exemption will not cause undue risk to BIDMC's IT Systems or Protected Data.
2. Exemption requests must be submitted to the CIO or his/her designee for triaging within BIDMC-IS.
3. Where practical, the User or technology representative will implement compensatory controls such as a heightened level of security monitoring to ensure the protection of BIDMC's Protected Data and Information Systems. Those controls will remain in place until the exemption is terminated.
4. BIDMC-IS periodically revisits exemptions to determine if they are still reasonable and appropriate in light of incidents that have arisen and the alternatives available for enhancing the security of the data.
5. BIDMC-IS develops a remediation plan for IT systems that are required to support a BIDMC business process but that are not in compliance with this policy as of the effective date.

BIDMC-IS Glossary of Terms

Definitions: Many of the terms used in this policy are defined by federal and state law. Except where an alternative definition is provided in this glossary, the legal definitions apply, as amended. The sources and key terms are listed below.

HIPAA (45 CFR Parts 160 and 164):

- § 160.103 – Business Associate, Disclosure, Electronic Protected Health Information, Use, Workforce;
- § 164.304 – Access, Administrative Safeguards, Authentication, Availability, Confidentiality, Encryption, Integrity, Malicious Software, Password, Physical Safeguards, Security or Security Measures, Security Incident, Technical Safeguards;

Breach Notification for Unsecured Protected Health Information regulations: (45 CFR Parts 160 and 164): § 164.402 – Breach, Unsecured Protected Health Information

Massachusetts data protection laws and regulations (MGL ch. 93H, 93I, 201 CMR 17.00): 201 CMR § 17.02 – Breach of Security, Electronic, Encrypted, Personal Information.

The following definitions are provided to clarify the meaning of certain terms used in this policy.

BIDMC-administered means Workstations, Mobile Devices or Electronic Media that is either BIDMC-owned or Grant-owned.

BIDMC-owned means Workstations, Mobile Devices or Electronic Media that is purchased with BIDMC capital funds, provided that BIDMC retains ownership of that equipment.

Breach (see "*Data Breach*")

Computer Information means all information and communications created, received, or stored on or passed through BIDMC's Information System. Computer Information includes but is not limited to all files, e-mail, application data and databases created or received by BIDMC Workforce Members as part of their job function.

Computer-Related Incident means an attempted or successful instance of the following:

a. The unauthorized or inappropriate access, use, disclosure, modification or destruction of electronic information; or

b. The interference with Information System operations that impairs the ability of Users to access electronic information; or

c. The theft or loss of media or a device which places the data stored thereon or the Information System at risk for the activities cited in paragraphs (a) and (b), respectively.

A Computer-Related Incident may result in an actual or suspected Data Breach.

Confidential or Proprietary Information may include material, in any form, related to the operation of BIDMC or a controlled subsidiary, including, but not limited to financial information, employee information, proprietary products and product development, marketing and general business strategies that are not intended by BIDMC for public disclosure, and information marked "confidential". Specific state and federal laws protect alcohol or substance abuse; sexually transmitted disease; and HIV status information.

Contingency Plan means a plan used by BIDMC or a particular BIDMC department or entity to respond to a specific systems failure or disruption of operations. The objective of the plan is to maintain or promptly restore computer operations, possibly at an alternate location, following such a failure or disruption.

Data Breach means the unauthorized acquisition, access, use or disclosure of Protected Data. In assessing whether a breach has occurred and whether notification is required, BIDMC considers, as required by law, whether the data was encrypted, security or privacy compromised, and the level of risk of identity theft or fraud by the person affected.

Disaster Recovery Plan means the management approved document that defines the resources, actions, tasks and data required by BIDMC-IS to manage the recovery effort following a major, usually catastrophic, event that denies access to the normal technology-related systems for an extended period. The plan may focus on restoring operability of the target system, application or computer facility at the primary or an alternate site following an emergency.

Electronic Protected Health Information ("EPHI") means protected health information (PHI) that is transmitted by or maintained in an electronic form.

Electronic Media means both storage and transmission media, in particular:

a. *Electronic Storage Media* includes, but is not limited to memory devices in Workstations or printers (hard drives) and any removable or transportable digital memory medium, such as magnetic tape or disk, optical disk, digital memory cards, USB thumb drives, digital music players, PDAs and smart phones that have the ability to store data; or

b. *Electronic Transmission Media* used to exchange information already in electronic storage media. Transmission media include but are not limited to the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks.

Electronic Transmission Media includes facsimile transmissions and telephone communications where the information being exchanged existed in an electronic form before the transmission.

Grant-owned means Workstations, Mobile Devices or Electronic Media that is funded by a research grant or research monies, provided that the equipment resides on BIDMC premises.

Inappropriate or Unlawful Content includes, but is not limited to:

a. Content that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate as determined by BIDMC in its sole discretion;

b. Content 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; and

c. Content that relates to gambling.

Information System means a set of resources that are interconnected, operating under the same management and sharing a common function. It may include but is not limited to hardware, software, information, data, applications and communications.

IT Workforce means Workforce Members whose work performance is controlled by:

a. BIDMC-IS; or

b. Another BIDMC department or entity and whose primary job function is the support and

maintenance of a component of BIDMC's Information System.

Management Sponsor means the BIDMC management official responsible for signing off on an access request for a User. That person must understand the nature of the job the User currently has and is responsible for determining the minimum access necessary for the User to perform that job.

Minimum Necessary means limiting the Protected Data used, disclosed or requested to the minimum necessary to accomplish the intended purpose or as necessary for the person to perform their job duties.

Mobile Device means portable storage media (e.g. USB memory sticks, external hard disk drives) and portable computing and communication devices with information storage capability (e.g. notebook/laptop computers, tablets, personal digital assistants (PDAs), cell phones, digital cameras and audio recording devices).

Personal Information ("PI") is defined by MGL ch. 93H as being a state resident's first and last name or first initial and last name and any one or more of the following data elements:

a. Social Security Number;

b. Driver's license number or state issued ID card; or

c. Financial account, insurance policy, credit or debit card number, with or without required security or other code that would permit access.

Recovery Point Objective ("RPO") means the point in time to which data must be restored in order to resume processing.

Recovery Time Objective ("RTO") means the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization.

Protected Data includes any data that is created, collected, processed, transmitted, stored or disseminated in any form (e.g. verbally, paper, electronic) and that must be secured in accordance with state or federal law (e.g. Protected Health Information (PHI), personal information (PI)). This policy, however, applies only to Protected Data that is in electronic form.

Users means all employees, system administrators, independent contractors, researchers, students, volunteers, consultants, contract employees, temporary workers, and other persons or entities that have authorized access to Protected Data and are authorized Users of the BIDMC Information System, wherever they are located. This term includes those who are not affiliated with BIDMC, but who use Workstations and telecommunications systems maintained by BIDMC. The term Users does not include BIDMC patients accessing PatientSite or members of the public accessing external BIDMC websites made available for that purpose.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions or uses active directory authentication services, and the Electronic Media stored in its immediate environment. Electronic media includes but is not limited to printers, scanners, audio devices or other output devices.

Workforce Member means employees, medical staff, volunteers, trainees, and other persons who perform work for BIDMC and whose work performance is under the direct control of BIDMC, whether or not they are paid by BIDMC.

IS Policy-Related Acronyms

Acronyms: The following list is provided to clarify the meaning of certain acronyms used in Information Systems-related policies.

BIDMC – Beth Israel Deaconess Medical Center

BIDMC-IS – BIDMC Information Systems Department

CIO – Chief Information Officer

CIR – Computer Incident Response Program

CISO – Chief Information Security Officer

CMR – Code of Massachusetts Regulations

EPHI – Electronic Protected Health Information

HIPAA – Health Insurance Portability and Accountability Act

MGL – Massachusetts General Laws

PDA – Personal Digital Assistant

PHI – Protected Health Information

PI – Personal Information

Vice President Sponsor: John Halamka, Sr. VP, Chief Medical Information Officer

Approved By:

☒ **Operations Council: 07/19/2010** **Eric Buehrens**
Chief Operating Officer

Requestor Name: John Halamka, Sr. VP, Chief Information Officer

Original Date Approved: 10/2001

Next Review Date: 07/2013

Revised: 07/07/2010

Eliminated:

References: