MCPHS UNIVERSITY
INFORMATION SECURITY PROGRAM

I. Program Overview

MCPHS UNIVERSITY ("MCPHS") has developed this comprehensive written information security program (the "Program") in order to create effective administrative, technical, and physical safeguards for the protection of Protected Information (defined below), and to comply with MCPHS's obligations under the Massachusetts regulations found at 201 C.M.R 17.00 *et seq.* (the "Regulations") and, where applicable, the General Data Protection Regulation (the "GDPR"), which governs the processing of personal data of residents of the European Union. This Program sets forth MCPHS's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing Protected Information.

For purposes of this Program, "Protected Information" includes, without limitation, a person's first name and last name, or first initial and last name, in combination with any one or more of the following data elements that relate to such person: (a) Social Security number, (b) driver's license number or state-issued identification card number, (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account, (d) birth date, (e) income tax information, (f) salary information, (g) student academic information, and (h) health information. "Protected Information" does not, however, include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public. "Protected Information" with respect to residents of the European Union to whom the GDPR applies (referred to herein as "GDPR Protected Information"), also includes any information related to an identified or identifiable natural person, including ID number and online identifiers (e.g., email address), together with indirect identifiers (such as location data). Also included in GDPR Protected Information are a person's biometric data, network identifiers, images, hobbies, political preferences, religious preferences, and sexual orientation.

This Program has been approved and adopted by MCPHS's Board of Trustees. This Program may be amended, suspended, or terminated from time to time by MCPHS, with the approval of the Board of Trustees**.**

II. Purpose and Scope

The purpose of this Program is to establish administrative, technical, and physical safeguards to protect Protected Information that is owned, licensed, stored, or maintained and, with respect to GDPR Protected Information, processed, by MCPHS, whether such information is contained in paper or electronic records (internal or cloud-based) or in any other form. This Program is designed to ensure the security and confidentiality of Protected Information in a manner consistent with industry standards, to protect against anticipated threats or hazards to the security or integrity of Protected Information, and to protect against unauthorized access to or use of Protected Information in a manner that creates a substantial risk of identity theft or fraud.

III. Administration of Information Security Program

A. Program Administration. MCPHS's Information Security and Compliance Committee (the "ISCC") will coordinate this Program. The names of the members of the ISCC and their contact information are set forth on MCPHS's Office of Compliance intranet web page.

B. Responsibilities of ISCC. The ISCC will be responsible, with the support of MCPHS and the Board of Trustees, to perform each of the following responsibilities, among others:

1. Identifying paper, electronic and other records, computing systems, and storage media, including cloud-based applications, laptops and portable devices used to store Protected Information, to determine which records contain Protected Information;

2. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of (a) any electronic, paper or other records containing Protected Information, and (b) cloud-based applications, including those administered by third-party service providers and mobile applications connecting to MCPHS's data assets, and evaluating and improving, where necessary, the effectiveness of the then current safeguards for limiting such risks;

3. Developing, implementing, administering, monitoring, reviewing, and upgrading this Program from time to time, consistent with the requirements of the Regulations and the GDPR to ensure that this Program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of Protected Information;

4. Overseeing ongoing employee training and any communications involving this Program;

5. Addressing any information security issues, including employee compliance and access to MCPHS's Protected Information by former employees, that may arise from time to time, and providing input to MCPHS regarding the imposition of disciplinary measures for violations of the Program; and

6. Taking all reasonable steps to verify that any third-party service provider with access to MCPHS's Protected Information has the capacity to protect such Protected Information in the manner consistent with this Program and the requirements of the Regulations and, where applicable, the requirements of the GDPR, and that any such third-party service provider applies protective security measures at least as stringent as those required by the Regulations and, where applicable, as those required by the GDPR.

C. GDPR Administration. A member of the MCPHS Information Security Department shall be designated as the Data Protection Officer for purposes of:

1. Coordinating responses to information security breaches with respect to GDPR Protected Information.

2. Overseeing employee training and communications involving protecting the security of GDPR Protected Information.

3. Overseeing responses to requests from persons who are EU residents with respect to their GDPR Protected Information.

IV. Compliance With Program

A. Compliance. All employees (whether full-time, part-time, substitute, seasonal, or temporary) and independent contractors, consultants, and volunteers (the "consultants and volunteers") are subject to the applicable requirements set forth in this Program.

B. Non-Compliance. Instances of non-compliance with this Program must be reported immediately to the ISCC. Violations may result in disciplinary action by MCPHS, up to and including termination of employment.

C. Non-Retaliation. It is unlawful and against MCPHS policy to retaliate against anyone who reports a violation of this Program or who cooperates in an investigation regarding non-compliance with this Program. Any such retaliation will result in disciplinary action by MCPHS, up to and including termination of employment.

V. Record Retention

A. Retention. MCPHS only collects and maintains records and files containing Protected Information of the type, and for the length of time, reasonably necessary to accomplish MCPHS's legitimate business purposes, or as otherwise necessary for MCPHS to comply with other local, state, or federal regulations or requirements. MCPHS periodically reviews its records, files, and form documents to ensure that MCPHS is not gathering and retaining Protected Information unless there is a compelling need to do so.

B. Return of Records. All employees, consultants, and volunteers of MCPHS are required upon termination or resignation from MCPHS for any reason, or earlier, if upon the request of MCPHS, to return or destroy all records and files containing Protected Information of current or former students, employees, or other service providers of MCPHS, in any form that may at the time of such termination be in their possession or control, including all such information stored on laptops, portable devices (such as thumb drives, zip drives, CDs, DVDs, cell phones, or blackberries), or other media, or in files, records, notes, or papers.

VI. Handling of Protected Information

Protected Information must be created, stored, disclosed, transmitted, and disposed of in the following manner:

A. Storage. Paper documents containing Protected Information must be stored in a locked or otherwise secured desk, file cabinet, office, or controlled area when unattended. Physical access to areas where Protected Information is stored or can be accessed must be restricted to only authorized MCPHS employees, consultants and volunteers.

B. Access, Sharing, and Disclosure. Access to, sharing, and disclosure of records or files containing Protected Information must be limited to those persons who are reasonably required to know such information in order to accomplish MCPHS's legitimate business purposes or to enable MCPHS to comply with other local, state, or federal regulations or requirements.

C. Transmission. Voice communications involving Protected Information must be kept to a minimum and performed in closed or secured locations. Transmission of Protected Information in paper or hard-copy form outside of MCPHS, or other removal of Protected Information from MCPHS's premises, must be done with reasonable precaution and in accordance with any applicable MCPHS procedures, policies and/or rules to ensure the security of such information and to prevent unauthorized disclosure. Transmission of electronic Protected Information on public networks must be encrypted, and must likewise be done with reasonable precaution to ensure the security of such information and to prevent unauthorized disclosure. Protected Information which is stored electronically must not be transferred to any personal computer, laptop or portable device which is not encrypted and supplied by MCPHS.

D. Disposal. Protected Information must be disposed of when no longer needed by MCPHS. Where appropriate, paper documents and other hard-copies of records or files containing Protected Information determined by MCPHS to be no longer needed should be disposed of by shredding, incineration, pulping, redaction, or burning, so that Protected Information cannot practicably be read or reconstructed. Electronic Protected Information determined by MCPHS to be no longer needed must be destroyed or erased so that Protected Information cannot practicably be read or reconstructed.

VII. Physical and Environmental Controls

A. Use and Storage of Files. Employees, consultants, and volunteers of MCPHS must not keep open documents or files containing Protected Information on their desks when they are not at their desks or in any other unsecured, unattended place. This policy applies to both hard-copies and electronic copies of records and files containing Protected Information. At the end of the work day, all files and other records containing Protected Information must be secured in a manner that is consistent with this Program and the requirements of the Regulations.

B. Blocked Physical Access. MCPHS prohibits and blocks physical access to records and files containing Protected Information by any individual without authorization to access such records as follows: (i) the MCPHS Department of Public Safety controls access to all MCPHS facilities in accordance with its Access Control policies and procedures, which policies and procedures are incorporated herein by this reference; (ii) each MCPHS department that has records and files containing Protected Information prohibits individuals without authorization to access such records from entering its physical space without supervision; (iii) any area containing Protected Information is secured by a locked door when not monitored by an individual with authorization to access Protected Information; and (iv) employees, consultants and volunteers of MCPHS are required, upon termination or resignation for any reason, or earlier if upon the request of MCPHS or the ISCC, to surrender all keys, IDs, access codes, badges, business cards, and the like, that permit access to MCPHS's premises or to records of MCPHS containing Protected Information.

C. Visitors. All visitors to MCPHS must be registered at the security desk upon entering and must be accompanied by an approved employee or other service provider of MCPHS. Visitors of MCPHS are prohibited and blocked from accessing any records or files of MCPHS containing Protected Information.

VIII. IT Policies and Procedures

A. Electronic Access.

1. MCPHS maintains secure user authentication protocols, including (i) control of user IDs and other identifiers, (ii) a reasonably secure method of assigning and selecting passwords; and (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect.

2. MCPHS assigns unique identifications plus passwords that are designed to maintain the integrity of the security of the access controls, and prohibits the use of vendor supplied default passwords, to each person with computer access.

3. MCPHS restricts access to authorized users and active user accounts only. Such restrictions allow access to records and files containing Protected Information only to users with a need to access such Protected Information in order to perform their job duties. MCPHS determines who shall be an authorized user with an active user account at MCPHS and which users need such information to perform their job duties.

4. MCPHS requires that current computer or network passwords are changed every ninety (90) days. MCPHS blocks access to users after multiple unsuccessful attempts to gain electronic access to records or files containing Protected Information.

5. MCPHS blocks electronic access to Protected Information by former employees, other former service providers of MCPHS, and other individuals who are no longer authorized users with an active user account.

6. MCPHS promptly terminates and prohibits electronic access by former employees, other former service providers of MCPHS, and other individuals who are no longer authorized users with an active user account to records and files containing Protected Information. Voicemail access, e-mail access, MCPHS internet access, and passwords are also promptly disabled or blocked.

B. Network Security.

1. MCPHS maintains reasonable monitoring systems for unauthorized use of or access to MCPHS records and files containing Protected Information.

2. MCPHS maintains reasonably up-to-date firewall protection and operating system security patches on all systems containing Protected Information that are reasonably designed to maintain the integrity of the Protected Information.

3. MCPHS maintains reasonably up-to-date versions of system security agent software which includes malware protection and reasonably up-to-date patches and virus definitions installed on all systems processing Protected Information and is set to receive the most current security updates on a regular basis.

C. Encryption.

1. To the extent technically feasible, MCPHS encrypts all records and files of MCPHS containing Protected Information transmitted across public networks or wirelessly.

2. MCPHS encrypts all Protected Information stored on laptops or other portable devices.

IX. Security Awareness and Training

A. Training. MCPHS provides education and training regarding this Program to all employees who will have access to Protected Information through their employment by MCPHS. Such education and training includes, without limitation, the proper use of the computer security system, the importance of Protected Information security, and remedial training as needed.

B. Consultants, Volunteers, Third-Party Service Providers. MCPHS communicates its relevant policies and procedures under this Program to its consultants, volunteers, and third-party service providers who will have access to Protected Information through their services to MCPHS.

X. Third-Party Service Providers

A. Vetting Process. MCPHS takes all reasonable steps to verify that any third-party service provider with access to MCPHS Protected Information has the capacity to protect such Protected Information in the manner provided for in the Regulations, and that any third-party service provider with access to GDPR Protected Information has the capacity to protect such GDPR Protected Information in the manner provided for in the GDPR.

B. Monitoring. MCPHS takes all reasonable steps to ensure that any third-party service provider with access to MCPHS Protected Information is applying to such Protected Information protective security measures at least as stringent as those required to be applied by the Regulations and, with respect to GDPR Protected Information, as those required to be applied by the GDPR.

XI. Risk Assessment and Incident Management

A. Identifying Records and Files Containing Protected Information. MCPHS shall regularly evaluate its paper, electronic, and other records, electronic systems, and storage media (including cloud-based applications, laptops and portable devices used to store Protected Information) to determine which records, files, and systems contain Protected Information.

B. Ongoing Risk Assessment. MCPHS shall, on a periodic basis, (i) conduct a review to identify reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of any electronic, paper, or other records containing Protected Information; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Protected Information; (iii) evaluate the sufficiency of this Program to control those risks; and (iv) revise this Program and safeguards to minimize those risks, consistent with the requirements of the Regulations. This risk assessment will include, but may not be limited to, an assessment of internal and external risks associated with ongoing employee training, employee compliance with this Program, and means for detecting and preventing security system failures.

C. Review of Program. MCPHS shall conduct a formal review of this Program at least annually, and whenever there is a material change in MCPHS's business practices that may reasonably implicate the security or integrity of records or files containing Protected Information.

D. Reporting Obligation. MCPHS requires that employees, consultants, and volunteers report any security violations, breaches of security, or suspicious or unauthorized use of Protected Information contained in records or files of MCPHS to the ISCC and, with respect to GDPR Protected Information, to the MCPHS Data Protection Officer.

E. Incident Review. MCPHS documents (i) responsive actions taken in connection with any incident involving a breach of security; and (ii) post-incident review of any such security incident and actions taken, if any, to make changes in business practices relating to protection of Protected Information.