Eskenazi Health
Confidentiality and Information Resource Agreement

As an employee, volunteer, student, physician, vendor, contractor or affiliate with system privileges at Eskenazi Health, you may have access to Confidential or electronic Protected Health Information (ePHI). You may also have access to, and use of, Eskenazi Health's Information Resources. In order to have access to Confidential information or ePHI, and to use Information Resources, you must adhere to this Agreement's provisions, which ensure security and provide the conditions of use. Additionally, this Agreement clarifies your duties and responsibilities under federal and state law, and Eskenazi Health policies.

1. DEFINITIONS:

Information Resources includes all Eskenazi Health hardware, software, data, information, network, personal computing mobile devices, phones, and other information technology.

ePHI includes any form of electronic protected health information.

Confidential or ePHI information, may include, but is not limited to:

a) Patient/member medical records (EMR), conversations, admitting data, financial records, and other records.
b) Employee information such as salaries, employment records, disciplinary action, personal demographics, and other records.
c) Business information such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source codes, proprietary technology, and other information.
d) Third party information such as computer programs, client and vendor proprietary information, source codes, technology, and other information.

2. USER RESPONSIBILITIES:

Confidential information, including ePHI, is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and any amendments, as well as applicable state laws, and Eskenazi Health policies. These laws and policies ensure that confidential information will remain confidential and will only be used for its intended purpose in order to accomplish the organization's mission.

In order to have access to Confidential or ePHI information, I understand that I must conduct myself in strict conformity with applicable laws and Eskenazi Health policies governing that information. This Agreement defines my principal responsibilities. I am required to read and abide by these responsibilities. My violation of any of these responsibilities may subject me to loss of system privileges, and/or disciplinary action, up to and including termination of employment and/or potential legal liability.

As a condition of, and in consideration for my access to such information, I agree to:

a.) Use Confidential information or ePHI only as needed to perform my legitimate duties as an employee, volunteer, student, physician, vendor, contractor or affiliate with system privileges at Eskenazi Health.

1. I will only access confidential information as required by my official duties;
2. I will not in any way divulge, copy, release, sell, loan, review, alter, or destroy any Confidential information or ePHI except as properly authorized within the scope of my

professional activities as an employee, volunteer, student, vendor, contractor or affiliate of Eskenazi Health;

3. I will not misuse or inappropriately download confidential information or ePHI;
4. I will take appropriate care to avoid the inappropriate use or misuse of confidential information or ePHI.

b.) I will be held accountable and liable for my misuse or wrongful disclosure of confidential information or ePHI as well as my failure to safeguard my user-IDs, passwords and/or other authorization to such information. Further, I accept responsibility for all activities undertaken using my user-ID or other authorization.

c.) I will use secure passwords that are not readily identifiable according to the system guidelines. For example, the names of my children, spouses, pets, and birth date are easily determined by individuals trying to access information unlawfully. It is further recommended passwords be a combination of letters, numbers and symbols.

d.) I will report activities by any individual or entity I suspect may compromise the confidentiality of any protected information.

e.) I understand my access privileges are subject to periodic review, revision, and, if appropriate, renewal.

f.) I understand I have no right to ownership interest in any confidential information or ePHI referred to in this Agreement. Eskenazi Health may at any time revoke my access code(s), other authorization, or access to confidential information or ePHI.

g.) In the event Eskenazi Health incurs any liability or expense as a result of my violation of this Agreement, I agree to reimburse Eskenazi Health for all such costs. Reimbursement provisions do not apply to employees/volunteers/students.

h.) If I am granted VPN access, or am authorized to work at a home, I understand any device I use must be current on operating system patches and have current virus and anti-spyware protection.

i.) If I am an employee, I understand my obligations under this Agreement will continue after termination of my employment.

3. APPROPRIATE USE:

a.) **Use for Eskenazi Health Business**. I understand that Information Resources are to be used solely to conduct the business of Eskenazi Health with exceptions limited to those provided by Eskenazi Health Policy 950-79.

b.) **Approved Information Resources.** I shall only use Information Resources owned, licensed, or being evaluated by the Eskenazi Health on the production network and shall not use personal or third party information resources, excluding cell phones, at Eskenazi Health facilities unless I have obtained prior written approval from my management and the Eskenazi Health Information Security Officer ("ISO"). For personal mobile devices I agree to comply with Eskenazi Health policy 950-214 Use of Mobile Devices.

c.) **Protecting from Misuse & Damage**. I shall use care in protecting Information Resources against unauthorized access, misuse, theft, damage, or unauthorized modification. I shall not leave a workstation without first ensuring it is properly secured from unauthorized access. I shall use good judgment to safely transport and store Information Resources in and away from the workplace.

d.) **Public Disclosure & Monitoring.** I understand that Eskenazi Health reserves the right to monitor any and all use of Information Resources, including my e-mail and Internet use, and I have no right or expectation of privacy with respect to my use of Information Resources.

e.) **Encryption.** I understand that before I transport any Eskenazi Health data, I must encrypt the data, laptops, tablets, and USB using the encryption technologies set forth in Eskenazi Health Policy 950-79.

f**.) Social Media.** If I use social media sites, I must protect the confidentiality and integrity of Eskenazi Health data. I may not post or transmit confidential or ePHI data including photographs via any Social Media technology.

g.) Compliance with Eskenazi Health policies. I agree to comply with all Eskenazi Health Information Technology policies including but not limited to 950-079 Acceptable uses of Electronic Devices Media and systems, 950-212 Social Media, and 950-214 Use of Mobile Devices.

4. PROHIBITED ACTIVITIES:

I understand that activities prohibited by this Agreement may not be permitted without the prior written approval of the Eskenazi Health ISO. Prohibited activities include:

a.)**. Downloads.** I shall not download and install any software, including privately purchased or free or shareware software, on Eskenazi Health owned devices.

b.) **Violation of Law.** I shall not use Information Resources to violate any law, including copyright or other intellectual property law. I shall not copy, share, or distribute software without authorization.

c.) **Unauthorized Use.** I shall not permit unauthorized users to use the Information Resources that Eskenazi Health has provided me. I shall promptly report any unauthorized use to my manager or the ISO. I shall not intentionally sustain high volume network traffic for non-business purposes which hinder others' use of the network and may increase Eskenazi Health costs.

d.) **Remote Access**. I shall not share confidential computer password(s) with any other person nor shall I use another person's confidential computer password(s). I shall not access or attempt to access information which I have no authorization or business need to access. I shall connect to the Eskenazi Health network only through approved services (e.g. – Citrix and VPN services are approved; a direct dial-up connection to a work PC modem is prohibited). I shall not use any remote control software or service on any internal or external host personal computers or systems.

e.) **Circumvention of Security Measures.** I shall not bypass or attempt to bypass measures in place to protect Information Resources from security threats and inappropriate use, including security tools such as sniffers, password crackers, peer to peer, remote control, and vulnerability assessment software. I shall not disable software on computing devices designed to protect Information Resources from malware (virus, WORM, etc.).

f.) **Unauthorized Devices**. I shall not place unauthorized computing or network devices on the Eskenazi Health production network.

g.) **Storage of Information.** I shall store Eskenazi Health owned information only on Eskenazi Health provided storage media. Storage of Eskenazi Health information on non-Eskenazi Health owned PCs, laptops, flash drives, CDs and other forms of media is prohibited. With appropriate authorization from my manager and the ISO, I am allowed to access and store Eskenazi Health email messages and business calendar on my personal cell phone or tablet.

h.) **Adherence to Security Guidance.** I shall ensure that protective measures are implemented promptly, as directed by Eskenazi Health, and that computing devices are connected to the network at least once per month to receive protective updates and patches.

i.) **Spam Awareness and Email Performance.** I shall be aware of the characteristics and dangers of spam messages. I shall not navigate to web links embedded in spam messages. I

shall not send or reply to messages that would negatively impact the performance of the email system (e.g. – "replying to all" on a message received in error).

j.) **Violations & Uncertainty.** I shall immediately report violations of this agreement to my manager or the ISO. If I am uncertain whether an activity is permissible, I will refrain from the activity and obtain authorization from my manager before proceeding.

k). **Eskenazi Health Social Media Sites.** I shall not create or develop Social Media sites that represent Eskenazi Health unless approved by the ISO and Public Relations in accordance with Eskenazi Health Policy 950-212 Social Media.

l.) **Changes and additional information.** I understand Eskenazi Health reserves the right to update this policy and will make reasonable efforts to inform me of the changes. I am held accountable to abide by the current version and any future updates.

By signing below, I certify that I am a (n):

_____ ***Employee*** _____ ***Physician***

_____***Researcher*** _____***Volunteer***

_____***Student*** _____ ***Vendor***

_____ ***Consultant*** _____ ***Other (please specify)***

Please provide a unique 4 digit pin to be used for verification purposes when resetting passphrases.

_____ **Pin**

and that I have read and understand the above <u>Confidentiality and Information Resource Agreement</u> and will comply with provisions.

and Upon your departure, Eskenazi Health may request that you affirm your obligations under this Confidentiality and Information Resource Agreement by signing a statement of understanding.

_____

Printed: Frist, Middle, Last

_____ _____

Signature **Date**

Revision History:

6-1-2011	**Original creation**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
1-2-2013	**Minor revisions updating for new policies**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
6-19-2013	**Revisions for 2014 Annual Education**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
01-02-2014	**Modified for Eskenazi Health added researcher as a category**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
01-02-2015	**Added 4 digit pin requirement**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
01-04-2016	**Annual Update**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
09-06-2016	**Annual Update**	**Frank A. Nevers, ISO/ HIPAA Security Officer**
01-03-2017	**Annual Update**	**Frank A. Nevers, ISO/ HIPAA Security Officer**