Eskenazi Health
Confidentiality and Information Resource Agreement

Eskenazi Health system users may have access to confidential information, including but not limited to employee information, financial information, business information and third-party information, as well as patient health information ("PHI") and electronic patient health information ("ePHI")[1] (all information referred to collectively in this Agreement as "confidential data"). This Agreement applies to all confidential data, regardless of the media or format, and regardless of how it is accessed. System users have no right of ownership in the confidential data, and Eskenazi Health reserves the right to monitor any and all system user activity, and to revoke system user access in its sole discretion.

In order to protect the privacy and security of Eskenazi Health's confidential data, system users must agree to the following terms and obligations before Eskenazi Health grants access. Please read the responsibilities carefully before agreeing to them by signing below:

1. I understand that in order to perform my employment, clinical, administrative, research–related, and/or other duties, I may be granted access to confidential data. I agree that privacy and security of confidential data is my personal duty and responsibility.

2. I agree that I will only use, access or disclose confidential data as minimally necessary for the purpose for which I have been granted access, including health care operations, treatment obligations, or approved research duties. I will not search for, view, access, change or use confidential data of friends, family members or others except as otherwise permitted (e.g., to perform my Eskenazi Health related or approved job duties).

3. I will not search for, view, access, change, or use my own PHI or ePHI, as this violates Eskenazi Health policy. Furthermore, I understand that I cannot use secure chat for my own (or my dependent's) personal health care. MyChart should be used to communicate with my provider.

4. At all times, I agree to take reasonable precautions to protect confidential data from unintentional or unauthorized access, use, alteration, disclosure, destruction, removal or theft.

5. I agree to use secure passwords, to protect my passwords, and not to disclose them to anyone else. I understand that I will be held accountable and liable for my misuse or wrongful disclosure of confidential data, as well as my failure to safeguard my user-IDs, passwords and/or other authorization to such data.

6. I will immediately report to my manager or the Eskenazi Health Director of Privacy any known or suspected data breaches, including theft of a mobile device containing confidential data or inappropriate use or access.

7. I agree to use, create, access, transmit or store confidential information using only approved equipment with encryption technology or equivalent appropriate protections. Storage of confidential information on non-Eskenazi Health devices (e.g., PCs, laptops, flash drives, CDs) and other forms of media is prohibited. With appropriate authorization and platform, I am allowed to access and store Eskenazi Health email messages and business calendar on my personal cell phone or tablet. However, it is impermissible to text patients or colleagues about patient care (including PHI) using my personal cell phone. See Eskenazi Health Policy 950-79.

[1] PHI and ePHI are used as defined by HIPAA.

8. If I receive VPN access, I understand any device I use must be current on operating system patches and have current anti-virus and anti-spyware protection.

9. I shall only use Eskenazi Health electronic devices or systems on the production network and shall not use personal or third-party devices, excluding cell phones, at Eskenazi Health facilities unless I have obtained prior written approval from my management and the Eskenazi Health Chief Information Security Officer ("CISO"). For personal mobile devices, I agree to comply with Eskenazi Health Policy 950-214 (Use of Mobile Devices).

10. I shall ensure workstations are properly secured from unauthorized access.

11. If I am uncertain whether an activity is permissible, I will refrain from the activity and obtain authorization from my manager or the CISO before proceeding.

12. I shall not download and install any software, including privately purchased or free or shareware software, on Eskenazi Health owned or leased devices or systems.

13. I shall not use Eskenazi Health owned or leased devices to violate any law, including copyright or other intellectual property law. I shall not copy, share, or distribute software without authorization.

14. I shall not permit unauthorized users to use the devices and systems that Eskenazi Health has provided me. 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.

15. 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.

16. I shall not bypass or attempt to bypass measures in place to protect Eskenazi Health devices or systems 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.).

17. I agree to complete relevant privacy and security training, and to comply with Eskenazi Health's privacy and security policies. I shall ensure that protective measures are implemented promptly, and that computing devices are connected to the network at least once per month to receive protective updates and patches.

18. 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). I will promptly submit any suspicious emails to Information Security via the Phish Alert Button ("PAB") within Outlook.

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 have read and understand the above Confidentiality and Information Security Agreement and will comply with provisions.

_____
Printed Name

_____ _____
Signature **Date**

_____
Eskenazi Health Employee ID

_____
If non-Eskenazi Health, identify affiliation

Please provide a unique challenge word to be used for identity verification purposes when contacting the service desk. This unique challenge word should be an easily remembered word (not a random collection of letters and number) that is not related to any of the user's personal information or password. Do not use the last four digits of the Social Security Number, mother's maiden name, child's name, pet's name, etc. Examples of a good challenge word may include words like "mirror", "console", blueberry", "shoe", etc.

_____ **Challenge Word**

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**
09-26-2018	**Modified**	**Julie M. Conrad, Chief Counsel**
9-5-2024	**Modified**	**René Wyatt-Foston, Senior Counsel and Privacy Director**