



Terms of Service (ToS)

Access to Wi-Fi:

The Aspire Guest wireless (Wi-Fi) network is a free public service provided by Aspire Indiana Health. Your access to the Aspire Guest Wi-Fi is completely at the discretion of Aspire Indiana Health, and your access to the service may be blocked, suspended, or terminated at any time for any reason including, but not limited to, violation of this Agreement, actions that may lead to liability for Aspire Indiana Health, disruption of access to other users or networks, or violation of applicable laws or regulations. Aspire Indiana Health may revise the ToS at any time. You must accept this Agreement each time you use the Service and it is your responsibility to review it for any changes each time. This is an open wireless network. No network communication is 100% secure.

Please remember: No Aspire Guest Wi-Fi network communication should be considered private or protected. All communication over the Aspire Indiana Health network is subject to monitoring. Aspire Indiana Health reserves the right to reduce throughput or access as need be.

Acceptable Use of the Service:

Your use of the Aspire Guest Wi-Fi and any activities conducted online through the Aspire Guest Wi-Fi shall not violate any applicable law or regulation or the rights of Aspire Indiana Health, or any third party. The following activities are strictly prohibited: Spamming and Invasion of Privacy of Others, Violating Intellectual Property Law, Transmitting Obscene or Indecent Speech or Materials, Transmitting Defamatory or Abusive Language, Hacking or Distribution of Internet Viruses, Worms, Trojan Horses, or Other Destructive Activities.

This facility handles HIPAA-regulated electronic protected health information (ePHI) and 42 CFR Part 2 substance use disorder (SUD) records, which require heightened protections.

Using Aspire Guest Wi-Fi, you agree that you will not:

- Attempt to access, view, intercept, disrupt, or “scan” any internal systems, devices, medical equipment networks, or restricted services.
- Transmit, store, or process patient information (including SUD treatment information) over this Guest Wi-Fi, especially if you are a contractor/vendor/visitor with any work-related access needs.
- Attempt any activity that could lead to unauthorized use or disclosure of regulated information (including prohibited re-disclosure expectations relevant to Part 2 information)

*(Workforce note: Aspire staff should use only approved, secured corporate connectivity and approved messaging platforms for any work involving ePHI/Part 2 data—**this guest network is not intended for that purpose.**)*

Disclaimer:

You acknowledge (i) that the Aspire Guest Wi-Fi may not be uninterrupted or error-free; (ii) that viruses or other harmful applications may be available through the Aspire Guest Wi-Fi; (iii) that Aspire Indiana Health does not guarantee the security of the Aspire Guest Wi-Fi and that unauthorized third parties may access your computer or files or otherwise monitor your connection.

Indemnity:

Under no circumstances shall Aspire Indiana Health, or affiliates, agents, or contractors thereof, be liable for any direct, indirect, incidental, special, punitive or consequential damages that result in any way from user’s use of or inability to use the Aspire Guest Wi-Fi or to access the Internet or any part thereof, or user’s reliance on, or use of information, services or merchandise provided on or through the Aspire Guest Wi-Fi, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation, or transmission, or any failure of performance. You agree to indemnify and hold harmless Aspire Indiana Health, including affiliates, agents, and contractors thereof, from any claim, liability, loss, damage, cost, or expense (including without limitation reasonable attorney’s fees) arising out of or related to your use of the Aspire Guest Wi-Fi, any materials downloaded or uploaded through the Aspire Guest Wi-Fi, any actions taken by you in connection with your use of the Aspire Guest Wi-Fi,

any violation of any third party's rights or a violation of law or regulation, or any breach of this agreement.

TCPA Compliance

Aspire leverages SMS enabled communication systems to connect and drive consumer engagement. When a consumer opts to allow Aspire to communicate with them via SMS they are also given the ability to opt out of SMS communication by way of a reply to the message of STOP or asking for the Aspire employee to remove them from the communication list. No mobile information will be shared with third parties/affiliates for marketing/promotional purposes. All the stated categories in this privacy policy exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties. To ensure SMS compliance for business-to-consumer communications, especially when involving patient health information (PHI), all Aspire employees will adhere to these key principles:

- Obtain explicit documented consent from recipients,
- Comply with the Telephone Consumer Protection Act (TCPA) to avoid unwanted messages,
- Safeguard patient privacy by strictly adhering to HIPAA regulations, including the Privacy Rule, Security Rule, HITECH Act, and Indiana-specific laws,
- Implement robust security measures to protect PHI, and
- Regularly review and update compliance policies and procedures to stay current with evolving regulations.

Statement programmed into initial SMS:

Consumer privacy is important to Aspire. ***“No mobile information will be shared with third parties/affiliates for marketing/promotional purposes. All the stated categories in this privacy policy exclude text messaging originator opt-in data and consent; this information will not be shared with any third parties. End users can opt out of receiving further messages by replying STOP or ask for more information by replying HELP. Message frequency varies. Message and data rates may apply. To review Aspire’s Privacy Policy visit this link [Privacy Policy](#)”***

Approved: VP-IS & IT 12/20/2024

Revised: VP-IS & IT 12/24/25