Notice of Cybersecurity Incident
September 10, 2026

Interim HealthCare is a home care and staffing provider. We recently experienced a limited cybersecurity incident at our corporate office that did not affect our franchise locations. This incident has been fully remediated, and it did not affect patient care or other services we provide. As detailed further below, we have confirmed that certain files used for monitoring patient care costs and quality assurance and care metrics were accessed during the incident. We are diligently reviewing the files to identify patient information involved and will send direct notices to patients when that review is complete. In the interim, we are providing this notice and sharing information on steps that patients may take while the review is ongoing.

What Happened? On July 13, 2026, we learned that a computer virus was installed on a limited portion of the corporate computer network. The function of this virus was to block access to our computer files, and then a cyber actor requests money in exchange for a software key to unlock the files. As noted above, this was installed on a limited portion of the corporate computer network, and it neither affected our corporate operations nor the operations of any of our healthcare locations. In response, we coordinated with cybersecurity specialists to confirm our network was secure and decommissioned the limited portion of the network involved to reduce the risk of an incident like this happening again.

During our investigation into this incident, we did learn that some files were copied from the computer network between July 9 and 11. Some of these files do contain high-level summaries related to patient care costs and quality assurance at some corporate care locations. We are working with a team of specialists to review these files to identify whose information is in them and will provide direct notices to patients whose information could be involved when that review is complete.

What Information Was Involved? This incident did not affect the electronic health records platform. However, certain care summaries are involved with this matter, and those include the following types of information: patient name, medical record number, treatment dates and care costs. Although the review is ongoing and we have not identified this information to-date, it is possible that corporate summaries may contain the following types of information: demographic information, such as address, contact information, date of birth, Social Security number, and driver's license or other government issued identifier; clinical information, including diagnosis, condition and treatment related information, lab results, and medications; and, financial information, including health insurance claims information, health insurance subscriber ID number, financial account number, and payment card number.

What We Are Doing. We are providing this notice to ensure patients are aware of this incident. We will also evaluate our cyber resiliency practices, including staff training, to reduce the risk of an issue like this reoccurring. We are also reporting this incident to the U.S. Department of Health and Human Services.

What Individuals Can Do. Whether patients wish to take any steps in response to this matter is a deeply personal decision. From files identified to-date, the information involved is high-level and does not create a risk of identity theft or fraud. Additionally, the files do not contain sufficient identifiers without access to other resources to actually identify patients. Nevertheless, we are mindful that the file review is ongoing and there could be files that contain detailed patient identifiers. For this reason, we are providing free resources and guidance in the *"Steps Individuals Can Take To Protect Personal Information"* and *"Steps Individuals Can Take to Protect Their Minor Dependents' Personal Information"* sections below. To the extent relevant information could be involved, we encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring their free credit reports for suspicious activity and to detect errors. Information on how to monitor free credit reports, place a fraud alert and/or security freeze on a credit file, and additional resources on how to monitor and protect against identity theft and fraud are located in the "*Steps Individuals Can Take To Protect Personal Information*" and "*Steps Individuals Can Take to Protect Their Minor Dependents' Personal Information*" sections below.

For More Information. If individuals have questions about this matter, we have an assistance line with agents ready to help answer those questions. You may contact our toll-free assistance line at 1-800-405-6108, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern Time (excluding U.S. holidays). Individuals may also write to us at Interim HealthCare, Attn: General Counsel, 1551 Sawgrass Corp. Pkwy, Ste. 230, Sunrise, FL 33323.

Thank you for your patience and understanding.

Sincerely,

Interim HealthCare Inc.

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Relevant Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

For loved ones that may have recently passed, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. Only one consumer reporting bureau needs to be notified, and it will notify the other two major consumer reporting bureaus. Individuals may complete this process using the information provided by the credit bureaus at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR MINOR DEPENDENTS' PERSONAL INFORMATION

Monitor Relevant Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor dependent has a credit report or to request a manual search for your minor dependent's Social Security number, each credit bureau has its own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit or contact the below credit bureaus.

Equifax: https://www.equifax.com/personal/education/identity-theft/articles/-/learn/child-identity-theft/; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian: https://www.experian.com/help/minor-request.html; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion: https://www.transunion.com/fraud-victim-resources; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

To request information about the existence of a credit file in your minor dependent's name, search for your dependent's Social Security number, place a security freeze on your dependent's credit file, place a fraud alert on your dependent's credit report (if one exists), or request a copy of your dependent's credit report you may be required to provide some or all the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor dependent's birth certificate;
- A copy of your minor dependent's Social Security card;
- Your minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor dependent's date of birth; and
- Your minor dependent's previous addresses for the past two years.

Additional Information

Individuals may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps individuals can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals and/or their minor dependent have the right to file a police report if their minor dependent ever experiences identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals or their minor dependent will likely need to provide some proof that their minor dependent has been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.