

How Proofpoint Protects the PHI of Pediatric Patients

Why cyber criminals target children's data and how to mitigate against fraudulent email attacks

Products

- Proofpoint Email Data Loss Prevention
- Proofpoint Email Encryption
- Proofpoint Security Awareness Training
- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response
- Proofpoint Browser Isolation

KeyBenefits

- Protect patient information
- Monitor and secure users' access to critical data
- Enable teams to rapidly respond to threat alerts
- Educate staff on safe cyber practices

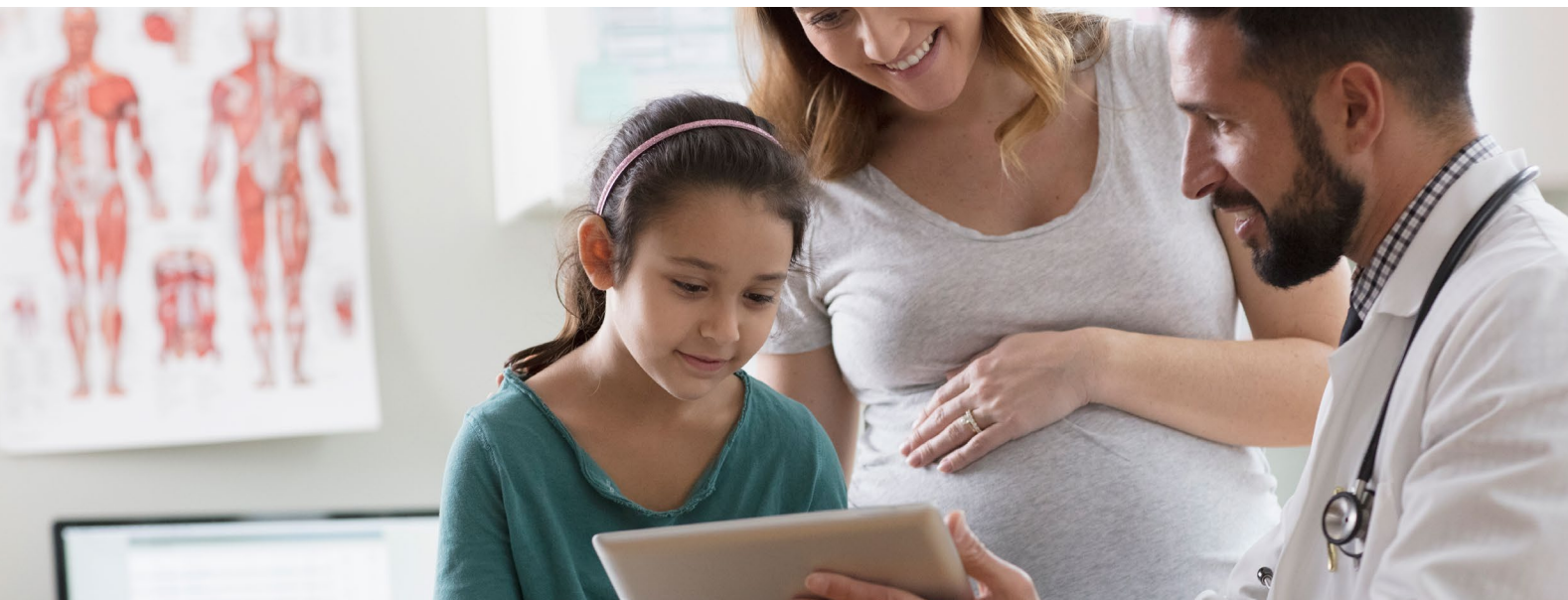
Children's hospitals and other pediatric healthcare institutions are inviting targets for cyber criminals. Highly sensitive children's health records are valuable on the black market for identity theft and monetary fraud. Children won't need to look at their credit report for up to 18 years. That leaves ample time for cyber criminals to maximize this stolen data usage. One thing is for sure—their primary way of breaching healthcare networks is through people—individual employees who are just trying to do their jobs. Proofpoint can help. Our cybersecurity and compliance solutions protect you, your staff and your patients.

Healthcare organizations are seeing more cyber attacks. They are an attractive target because they have two kinds of valuable data:

- Highly sensitive electronic medical records (EMRs)
- Financial information about young patients

Both categories of data can bring big profits for cyber criminals.

When bad actors steal this information, institutions can lose money in several ways. Compliance fines can be assessed. And litigation by victims can lead to large settlements. Moreover, reputational damage can have long-term impacts on the bottom line. Patients, for their part, can be affected by identity theft and fraudulent financial activity. But the impact can go far beyond the financial. Compromised EMRs and medical devices can have a devastating impact on the quality of care and patient safety.



Pediatric institutions have unique challenges because of their clientele. Children and teenagers whose personal data is compromised can suffer ongoing financial losses. Besides, bad impacts on the quality of care can hamper their growth and development during their formative years.

Most hospitals use email to communicate with off-site care teams and insurance companies about patients. But email is also the key route that cyber criminals use to get into your pediatric healthcare organization.

According to the 2020 HIMSS Cybersecurity Survey, 89% of respondents had a significant security incident for which email was the initial point of compromise.¹ The same report cited email phishing of all types as the “primary means for compromising systems and networks.”

The misuse of children’s medical and financial data has a wide range of bad outcomes for your patients and your institution. It is everyone’s responsibility at your pediatric institution to protect that information. Financial impacts are compounded by:

- Threats to patient safety
- The quality of care
- The overall well-being of children everywhere

Pediatric Healthcare Cybersecurity Challenges

Children’s healthcare institutions take many steps to protect patient and corporate data. But they face many challenges along the way. Complexity is the name of the game in 2021. People’s lives will gradually return to some semblance of “normal.” But many of the abrupt changes that occurred in 2020 are here to stay.

¹ HIMSS. “2020 HIMSS Cybersecurity Survey.” November 2020.

Remote workers and remote care

Precautions compelled by COVID-19 have abruptly transformed how all healthcare institutions deliver care. For example:

- Providers now conduct more virtual appointments²
- Much of the non-clinical staff, like those who manage electronic medical records (EMRs), research data and patient financial information, work from home³

These work arrangements will not suddenly end when COVID-19 is under control.⁴

As always, cyber criminals have adapted their tactics to take advantage of these changes.⁵ As children's hospitals move beyond the network perimeter, so do attackers. And their tactics reflect the anxiety brought about by the pandemic. COVID-19-themed phishing emails began to appear almost immediately.⁶ And messages have been adjusted over time based on current events.⁷

Financial identity theft and fraud

Like most hospitals, children's hospitals handle a large volume of highly sensitive information on their patients—both medical and financial. Sadly, children are one of the most sought-after targets for financial identity theft.⁸

Your minor patient's personally identifiable information (PII) is worth its weight in gold on the black market. Most children have not established a credit history. Besides, they won't be applying for loans or credit cards any time soon. Bad actors know that most parents aren't checking to see if this data is being misused or used for fraud. This gives them years to benefit from the data they have stolen.

Medical identity theft and fraud

A young patient's protected health information (PHI) can be used for medical identity theft and fraud. It could have long-term safety and health impacts on these vulnerable pediatric patients.⁹ For example:

- Cyber criminals can use your patient's PHI to file claims with insurance companies for doctor's visits and prescription drugs for someone else.
- Incorrect information can be entered into the child's EMR and this can result in harmful medications or treatment being administered later on. This could have long-lasting safety and health impacts on your pediatric patients.

Research integrity and intellectual property

Clinical trials and other research at pediatric institutions are especially vulnerable. Medical research with children is challenging under the best of circumstances.¹⁰ Because of this, children are greatly underrepresented in clinical research around the world.

2 Centers for Disease Control and Prevention. "Trends in the Use of Telehealth During the Emergence of the COVID-19 Pandemic — United States, January–March 2020." October 2020.

3 Relias Media. "HIPAA Compliance a Concern as Working from Home Becomes Norm." September 2020.

4 Jennifer Radin and Casey Korba (Deloitte Insights). "COVID-19 as Catalyst: The Future of Work and the Workplace in Health Care." November 2020.

5 Danny Palmer (ZDNet). "Coronavirus and Home Working: Cyber Criminals Shift Focus to Target Remote Workers." March 2020.

6 Phil Taylor (*PharmaForum*). "COVID-19-Themed Cyber Attacks Hit Healthcare Bodies." April 2020.

7 Jessica Davis (*Health IT Security*). "COVID-19-Related Phishing Lingers, as New Attacks Use Vaccine Themes." December 2020.

8 Herb Weisbaum (*NBC News*). "More than 1 Million Children Were Victims of ID Theft Last Year." June 2018.

9 Federal Trade Commission. "Medical Identity Theft." Accessed March 3, 2021.

10 Worldwide Clinical Trials. "Overcoming the Challenges of Pediatric Clinical Research." April 2020.

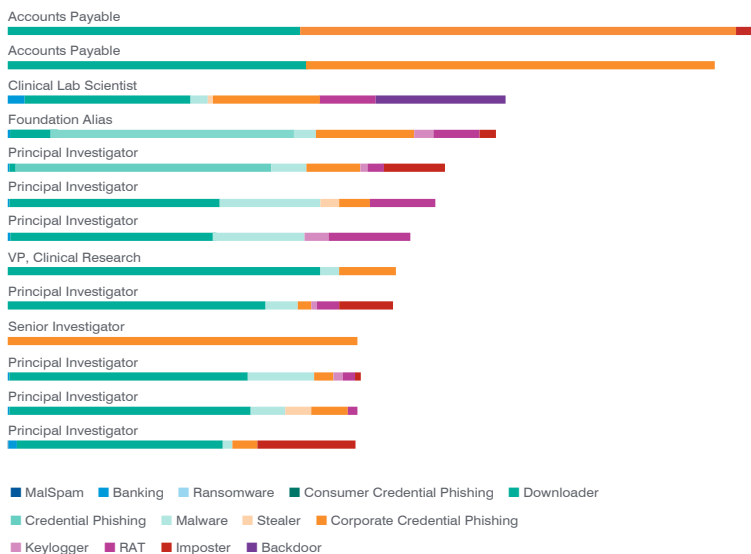


Figure 1: Breakdown of Very Attacked People at a prestigious children’s hospital.

If research data is compromised, it could spoil a trial. Or it could even endanger its participants. This could set back the research into lifesaving treatments by years. Even if the research data is salvaged, cyber criminals can continue to disclose your intellectual property to competitors.

Quality of care and patient safety

The financial impacts described here can adversely affect your patients and your organization. But saving lives and restoring health is far more important than finances. When a cyber attack compromises medical devices, healthcare applications or EMRs, life-and-death safety impacts can result.

Taking a People-centric Approach

These days, cyber attacks target people, not technology. Because of this, your children’s healthcare organization must take a people-centered approach to secure your sensitive data. Clinical workers, non-clinical staff and researchers have access to different kinds of data to do their jobs. This information must be available quickly. When providers communicate with outside parties to coordinate a patient’s care, they often use email. And as they care for multiple patients and deal with emergencies, the legitimacy of an email is far from the top of their mind.

Our 2020 Healthcare Threat Landscape report explores what we call Very Attacked People™ (VAPs) in healthcare. We use this term to define the most heavily targeted employees within an organization. Figure 1 shows a real-life example from a children’s hospital based on Proofpoint telemetry.

In addition to this data from real pediatric institutions, we recently conducted another focus group discussion. We engaged IT security leaders at children’s healthcare

organizations around the country. They confirmed much of the story that we find in our internal data. They said that job titles in the research department are highly attacked. Just like the “investigator” titles in our example. Also, the hospital’s foundation alias is another popular target.

Researchers handle large amounts of patient data. That includes research IP and financial data from government loans and grants. And research is commonly shared and collaborated among third parties. That leaves researchers prone to large volumes of phishing or impostor attacks. At most large hospitals privacy concerns are heightened because pediatric data is a popular target. Hospital foundations are another popular target. They deal with fundraising and community awareness. That makes them an easy target for phishing or impostor attacks.

But the children’s hospital leaders we interviewed agreed that those who handle financial data are at the top of the list. The accounting department manages confidential financial information from patients, insurance companies and employees. That’s a gold mine of valuable data to exploit.

How Proofpoint Can Help

Proofpoint gives pediatric institutions the tools they need to protect their people. And that includes clinical staff, researchers and those who process financial and insurance transactions. We can help you in a variety of ways, as described below.

PHI protection: Keeping patients’ data safe

As we have pointed out, cyber criminals use email more than any other vector to attack people in healthcare. The right email data loss prevention (DLP) solution ensures that only

authorized people can access different types of sensitive and business-critical information.

With Proofpoint people-centric DLP, your children's healthcare institution can identify and respond quickly to data risks such as those posed by negligent, compromised and malicious users. Our unified platform allows customers to define different categories of data. It lets you:

- Leverage these definitions across the entire platform
- Protect the confidentiality of individual email messages through Proofpoint Email Encryption
- And your user community can trigger encrypted messages automatically by adding a keyword of choice to the subject line, or trigger message-level encryption based on DLP rules

Distributed health security

As they coordinate their patients' care, pediatric institutions must coordinate, collaborate and share with other organizations and IT networks. Communication with patients and their families is also critical. Email is a popular method of sharing confidential information. And most high-profile healthcare data breaches begin with targeted phishing attacks. Proofpoint protects children's hospitals by protecting users in the way they work today with:

- **Proofpoint Email Protection.** Delivers top-rated email security to stop malware and non-malware threats.
- **Proofpoint Data Loss Prevention.** Mitigates the risk of email data loss and protects against email fraud.
- **Proofpoint Targeted Attack Protection (TAP).** With sandboxing capabilities detects and stops advanced threats.
- **Proofpoint Threat Response.** Responds quickly to resolve threats.
- **Proofpoint Security Awareness Training.** Provides employees training to spot healthcare-themed social engineering attacks, such as sophisticated phishing ploys.

Secure care collaboration

Clinical staff at pediatric hospitals need effective collaboration and communication at the point of care. They have mobile solutions that connect clinicians and patients. But they are built for function and convenience and not for security. They are often used outside the protected enterprise network. Physicians access clinical applications from personal devices too. And at the same time, they may use personal email accounts on corporate-issued hardware.

Proofpoint Browser Isolation keeps users' personal activity and harmful content out of your environment. It insulates webmail and any URLs it holds within a protected container. Users can access their personal accounts freely and privately through their usual web browser. But potentially harmful content and actions are disabled, so your environment stays safe.

Conclusion

Pediatric healthcare organizations provide lifesaving care to vulnerable children. And we give them protection and visibility for their greatest cybersecurity risk—their people. Whether they are targeted through email, the web, social media or cloud apps, we have the solution. We provide the most effective cybersecurity by protecting those interactions. And we stop threats before they reach clinical and support staff. This helps safeguard your valuable data. And it protects your vulnerable patients from cyber attacks.

Leading healthcare organizations of all sizes rely on us to prevent, detect and respond to cyber attacks before they cause lasting harm. This includes five of the top 10 ranked in the 2020–21 Best Children's Hospitals Honor Roll from *U.S. News and World Report* trust Proofpoint to protect their staff and patients.¹¹

LEARN MORE

For more information, visit [proofpoint.com](https://www.proofpoint.com).

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners. Proofpoint.com