Vulnerability Disclosure Policy

Responsible Disclosure:

Children's Minnesota is committed to maintaining the trust and confidence that our patients and their families place in us. Therefore, the security of our patient web site and maintaining patient privacy are of utmost importance to us. If you are a security researcher and have discovered a security vulnerability in one of our services, we appreciate your help in disclosing it to us in a responsible manner. Children's Minnesota will engage with security researchers when vulnerabilities are reported to us in accordance with this Responsible Vulnerability Disclosure Policy. We will validate and fix vulnerabilities in accordance with our commitment to security and privacy. We will not take legal action against those who discover and report security vulnerabilities following the terms of this Responsible Disclosure Policy. Children's Minnesota reserves all legal rights in the event of any noncompliance.

Reporting:

We encourage security researchers to share the details of any suspected vulnerabilities with the Children's Minnesota Information Security Office by submitting the form at the bottom of this page]. Children's Minnesota will review the submission to determine if the finding is valid and has not been previously reported. Children's Minnesota's is extremely thankful for those who report vulnerabilities, but our policy as a non-profit organization is to provide no monetary compensation for your efforts. We require security researchers to include detailed information with steps for us to reproduce the vulnerability.

Children's Commitment:

If you identify a valid security vulnerability in compliance with this Responsible Disclosure Policy, Children's Minnesota commits to:

- Work with you to understand and validate the issue
- Address the risk if deemed appropriate by Children's Minnesota team

Prohibitions:

Public disclosure of the submission details of any identified or alleged vulnerability without express written consent from Children's Minnesota will deem the submission as noncompliant with this Responsible Disclosure Policy. In addition, to remain compliant, you are prohibited from:

- accessing, downloading, or modifying data residing in any account that does not belong to you;
- retaining any Children's data that was accessed during vulnerability testing;
- accessing data or performing any activity that would be disruptive or damaging to any Children's Minnesota patients or patient families;
- executing or attempting to execute any Denial of Service attack;

- conducting social engineering experiments to acquire information from Children's workforce;
- posting, transmitting, uploading, linking to, sending, or storing any malicious software;
- testing in a manner that would result in the sending of unsolicited or unauthorized junk mail, spam, pyramid schemes, or other forms of duplicative or unsolicited messages;
- testing in a manner that would degrade the operation of any Children's Minnesota properties;
- testing third-party applications, websites, or services that integrate with or link to Children's Minnesota properties.

Please use the Website Vulnerability Form to report any vulnerabilities.