HB Healthcare Safety, SBC Vulnerability Disclosure Policy

HBHS is committed to the security and protection of our products, services, customer data, and infrastructure.

We appreciate a responsible submission if you believe you've found a security vulnerability in an HBHS product. You can submit a detailed description of the issue to us, including the steps that we can take to reproduce the issue and/or a proof-of-concept ("Report").

We ask that reporters honor responsible disclosure principles and processes while engaging with us for HBHS to evaluate, respond to, or remediate any confirmed security vulnerabilities before public or third-party disclosure.

Responsible Reporting and Disclosure

HBHS believes in responsible reporting and disclosure, and we ask the following:

- Promptly report the vulnerability to us and provide as much detail so we can reproduce the vulnerability.
- Report the details of the security vulnerability to us without sharing any information of the vulnerability publicly.
- Do not access, modify, destroy, or violate the privacy of any HBHS customer or data.
- Comply with all applicable laws.
- Avoid degradation of user experience, disruption to production systems, and any access, copying, destruction, or manipulation of data.
- Once you've established that a vulnerability exists or encountered any of the sensitive data outlined below, you must stop your test and notify us immediately.
- You will NOT be executing, or attempting to execute, a denial-of-service (DoS) attack.

Scope

This policy applies to all the products, services, and infrastructure developed, managed, and maintained by HBHS.

Rules of Engagement

Certain vulnerabilities are considered out of scope and include the following:

- Physical attacks against infrastructure, facilities, offices
- Social engineering attacks, including those targeting our employees, contractors, vendors
- Denial of Service attacks or any activity leading to the disruption of our service
- Any vulnerability obtained from a compromised account
- Scanner output or scanner generated reports
- User Interface or bugs
- Network vulnerabilities (e.g., account takeover, spam, clickjacking, fingerprinting)
- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Rate limiting or brute force issues on non-authentication endpoints
- Phishing attacks
- Issues that require unlikely user interaction.
- Testers will not modify the “Authentication” page of any designated testing Org.
- Testers will limit testing to the URLs/Orgs provided.

If you encounter any of the below on HBHS systems while testing within the scope of this policy, stop your test and notify us immediately:

- Personal Identifiable Information (PII)
- Customer Data or Account Credentials
- Financial information (e.g., credit card or bank account numbers)
- Proprietary information or trade secrets of companies of any party
- Denial of Service or situations where the site and application are not responding

Reporting a Security Vulnerability

If you believe you have discovered a security vulnerability issue, please share the details with HBHS by emailing security@hbhealthcaresafety.com the following

Subject: HBHS Security Vulnerability - <Title>
Body:

<URL>
<Summary>
<Attachments as needed>

HBHS will try to acknowledge receipt of your report within 2 business days, provide you with an estimated timetable for resolution of the vulnerability, notify you when the vulnerability is fixed, and, with your permission, publicly acknowledge your responsible disclosure.

Email communication between you and HBHS, including without limitation, emails you send HBHS reporting a potential security vulnerability, should not contain any of your proprietary information. The contents of all email communication you send to HBHS shall be considered non-proprietary. HBHS, or any of its affiliates, may use such communication or material for any purpose whatsoever, including, but not limited to, reproduction, disclosure, transmission, publication, broadcast, and further posting.

Further, HBHS and its affiliates are free to use any ideas, concepts, know-how, or techniques contained in any communication or material you send to HBHS for any purpose whatsoever, including, but not limited to, fixing, developing, manufacturing, and marketing products. By submitting any information, you are granting HBHS a perpetual, royalty-free and irrevocable right and license to use, reproduce, modify, adapt, publish, translate, distribute, transmit, publicly display, publicly perform, sublicense, create derivative works from, transfer and sell such information.

Legal

HBHS is unable to award a bounty to reporters who reside in a country that has been deemed sanctioned by the United States. HBHS employees or previous employees (within the last six months), contractors, and their family members are not eligible for bounties.

Questions

For any questions on the policy and for further help, please write to us at security@hbhealthcaresafety.com

Note: HBHS reserves the right to update the policy at any time.