Comprehensive Testing Feedback Report: Global Health Works Platform

Application: Global Health Works (https://globalhealth.works/)
Testing Scope: User Authentication & Registration Flows, Dashboard Content
Report Date: February 2, 2026
Testing Environment: Production Web Application, all modern browsers

---

Executive Summary

A comprehensive review of the Global Health Works platform revealed multiple issues impacting user experience (UX), data integrity, and security posture. The findings span from cosmetic content errors to critical flaws in form validation and application navigation logic. Addressing these issues is essential to ensure a professional, secure, and frictionless user onboarding experience.

The most critical issues identified include a broken OTP verification flow that forces users backward in the sign-up process, lack of password confirmation during registration, and weak password validation that permits insecure credentials. Immediate attention to these high-priority items will significantly reduce user drop-off and support overhead.

Detailed Findings

1. Authentication & Sign-up Flow Issues (High Priority)

1.1. Missing Critical "Confirm Password" Field

Bug ID: AUTH-SIGNUP-FLOW-002

Issue: The sign-up form requires users to enter their password only once, with no "Confirm Password" field to verify the entry and catch typing errors.

Impact: High. Users who mistype their password have no opportunity to catch the error before account creation, leading directly to account lockout, failed login attempts, and increased password reset requests.

Steps to Reproduce:

1. Navigate through the sign-up flow to the password creation step
2. Observe only a single "Password" input field is present
3. No "Confirm Password" or "Re-enter Password" field exists

Recommendation: Add a mandatory "Confirm Password" field with real-time validation that blocks form submission until both password fields match exactly. Display a clear error message ("Passwords do not match") when values differ.

1.2. Weak and Inconsistent Password Validation Logic

Bug ID: AUTH-PASSWORD-POLICY-001

Issue: The password strength validator exhibits inconsistent, confusing behavior and lacks essential security requirements.

Specific Problems:

- **No minimum length requirement** - accepts passwords as short as one character
- **Incorrect strength assessments** - labels "pass123" (lowercase + numbers only) as "Good" and "pass1234" as "Strong"
- **Contradictory feedback** - suggests "add one more number" when a number is already present
- **Incremental rather than comprehensive validation** - does not enforce all complexity rules simultaneously

Examples of Problematic Behavior:

- Input: `a` → "Weak password, try adding uppercase letters, numbers, and a symbol." (No mention of critically short length)
- Input: `pass123` → "Good password strength, add one more symbol or number for extra security." (Missing uppercase and symbols, yet rated "Good")
- Input: `pass1234` → "Strong password, this password is quite secure." (No uppercase or symbols, incorrectly rated "Strong")
- Input: `@icY` → "Good password strength..." (Only 4 characters, rated "Good")

Impact: Medium-High. Allows creation of weak, easily compromised passwords. Confusing messaging undermines user confidence and fails to guide proper password creation.

Recommendation: Implement a clear, enforced password policy that validates all requirements simultaneously:

- **Minimum 8 characters**

- **At least one uppercase letter (A-Z)**
- **At least one lowercase letter (a-z)**
- **At least one number (0-9)**
- **At least one special character (e.g., ! @ # $ % ^ &)*

Display all five requirements with real-time visual indicators (checkmarks/X marks) and block submission until all criteria are met.

1.3. Inadequate Email Address Validation

Bug ID: AUTH-EMAIL-VALIDATION-002

Issue: Email validation only checks for the presence of an "@" symbol, accepting structurally invalid email formats.

Invalid Formats Currently Accepted:

- `g@w` - Missing top-level domain (TLD) and dot separator
- `test..@gmail.com` - Consecutive dots in the local-part (before @)

Impact: Medium. Results in 100% email delivery failure for verification messages, OTPs, and notifications. Creates poor user experience and clutters the database with invalid data.

Steps to Reproduce:

1. Enter `g@w` in the email field → Accepted
2. Enter `test..@gmail.com` in the email field → Accepted

Recommendation: Implement comprehensive email format validation using a standard regex pattern that enforces:

- Proper structure with local-part @ domain.TLD
- No consecutive dots
- No missing domain components

Suggested pattern: `^[^\s@]+(?:\.[^\s@]+)*@[^\s@]+\.[^\s@]+$`

1.4. Misleading Login Error Message for Non-Existent Accounts

Bug ID: AUTH-LOGIN-MESSAGING-001

Issue: When a user attempts to log in with an unregistered email address, the system displays the generic error "Invalid credentials." This message is ambiguous and does not differentiate between "wrong password for existing account" and "account does not exist."

Impact: Medium. Users cannot determine the root cause of login failure, leading to repeated failed attempts, unnecessary password reset requests, and frustration. Users without accounts may not realize they need to sign up.

Steps to Reproduce:

1. Navigate to the login page
2. Enter an email address not registered in the system
3. Enter any password
4. Observe the error: "Invalid credentials"

Recommendation: Provide clearer, more actionable messaging while balancing security considerations:

- **Preferred approach:** "The email or password you entered is incorrect. Please try again or [Sign Up]."
- **Alternative:** If user clicks "Reset Password" for a non-existent account, then show: "We couldn't find an account with that email. Please [Sign Up]."

This guides users toward the correct action without explicitly confirming whether an email exists (avoiding email enumeration vulnerabilities).

1.5. Critical Navigation Bug in OTP Verification Flow

Bug ID: PLATFORM-SIGNUP-NAVIGATION-001

Issue: On the "Enter OTP Code" verification screen (Screen 3), clicking the "Resend OTP" link incorrectly navigates the user two steps backward to Screen 2 (Organization Details) instead of remaining on the OTP screen.

Impact: High. This completely breaks the verification workflow, forces users to re-enter organizational information, and will cause significant sign-up abandonment. This is a critical functional blocker.

Steps to Reproduce:

1. Complete Screen 1 (Personal Details) and Screen 2 (Organization Details)
2. Arrive at Screen 3 (Enter OTP Code)
3. Click the "Resend OTP" link
4. Observe incorrect navigation back to Screen 2

Expected Behavior:

- Send a new OTP code to the user's email
- Display confirmation message: "A new code has been sent to your email."
- **Keep user on Screen 3** with any partially entered code preserved

Recommendation: Fix the navigation logic immediately. The "Resend OTP" action must only trigger the OTP resend API call and provide user feedback, without any navigation events. This appears to be a deep navigation stack error.

---

2. Sign-up Form & Data Quality Issues (Medium Priority)

2.1. Missing "Optional" Field Indicators

Bug ID: SIGNUP-FORM-UI-001

Issue: In the Task Owner sign-up flow, the fields "Short Bio" and "Professional Link (LinkedIn, website, etc.)" are optional but lack any visual indicator to communicate this to users. They appear identical to mandatory fields.

Impact: Low-Medium. Creates unnecessary friction in the registration process. Users may:

- Abandon sign-up, believing they must provide information they're unprepared to share
- Provide rushed, low-quality information
- Experience hesitation and confusion

Recommendation: Add the text **(Optional)** in a subtle secondary style next to the field labels:

- "Short Bio **(Optional)**"
- "Professional Link (LinkedIn, website, etc.) **(Optional)**"

Apply this pattern consistently across all optional fields in the application.

2.2. Insufficient "Organization Name" Field Validation

Bug ID: SIGNUP-VALIDATION-ORGNAME-001

Issue: The "Organization Name" field in the Task Owner sign-up accepts input as short as a single character (e.g., "A", "1", "-").

Impact: Low-Medium. Allows nonsensical, low-quality data into a key profile field. Organization names are likely displayed publicly on tasks and profiles, and single-character names appear unprofessional and reduce platform credibility.

Steps to Reproduce:

1. In the "Organization Name" field, enter a single character
2. Proceed to the next screen - input is accepted

Recommendation: Enforce a minimum character length of at least 2-3 characters. Display an error message if validation fails: "Organization name must be at least [X] characters long."

---

3. Content & Presentation Errors (Low Priority)

3.1. Testimonial Typo on Dashboard

Bug ID: WEB-CONTENT-TYPO-001

Issue: In the "What Our Users Say" section on the dashboard, the testimonial from Dr. Maria Santos (Pediatrician, Brazil) - the third testimonial card - is missing the first letter "T".

Current Text: "his platform bridges the gap between health challenges and those ready to solve them. A brilliant initiative!"

Correct Text: "**T**his platform bridges the gap between health challenges and those ready to solve them. A brilliant initiative!"

Impact: Low. Cosmetic error that affects professional presentation and content accuracy.

Recommendation: Correct the testimonial text by adding the missing "T".

3.2. Spelling Error in Account Pending Approval Message

Bug ID: AUTH-MESSAGING-TYPO-001

Issue: The informational message displayed to users with pending accounts contains a spelling error: "memebers" instead of "members".

Current Text: "To maintain the integrity of our network and ensure the security of all **memebers**, our team manually reviews every new account..."

Correct Text: "To maintain the integrity of our network and ensure the security of all **members**, our team manually reviews every new account..."

Impact: Low. While functionality is unaffected, spelling errors in official security-related communications can slightly undermine perceived professionalism and trustworthiness.

Recommendation: Correct the spelling error.

Priority Summary

Priority Level	Issues	Count
High	Missing "Confirm Password" field, OTP Resend navigation bug	2
Medium-High	Weak/inconsistent password validation logic	1
Medium	Inadequate email validation, misleading login error message	2
Low-Medium	Missing optional field labels, insufficient "Organization Name" validation	2
Low	Dashboard testimonial typo, spelling error in system message	2

Total Issues Identified: 9

General Observations & Recommendations

1. Validation Consistency

There is a clear pattern of insufficient front-end validation across the sign-up form (password strength, email format, organization name length). Implementing a consistent, robust validation framework with clear error messaging across all input fields is strongly recommended.

2. User Journey Integrity

The OTP navigation bug is particularly severe as it disrupts a critical, time-sensitive user task during account creation. This should be treated as the highest priority fix, as it directly blocks successful user onboarding.

3. Security Posture

The combination of weak password validation and missing password confirmation creates a security-adjacent risk. While not a direct vulnerability, these issues encourage poor password practices and increase the likelihood of account compromise or lockout.

4. Clarity Over Ambiguity

Error messages (e.g., "Invalid credentials") and field requirements (optional vs. required) should be explicit and actionable. Clear communication reduces user confusion, decreases support burden, and improves overall conversion rates.

5. Professional Polish

While content typos are low severity individually, they accumulate and can affect the perceived credibility of a platform operating in the professional global health sector. Given the platform's mission to connect health professionals and organizations, maintaining high editorial standards is important for trust-building.

Conclusion

The Global Health Works platform demonstrates a solid foundation and clear value proposition. However, the user onboarding and authentication flows require focused attention to ensure a smooth, secure, and professional experience.

Immediate Action Items:

1. Fix the OTP Resend navigation bug (critical blocker)
2. Add "Confirm Password" field to registration
3. Implement comprehensive password policy with clear requirements

Short-term Priorities: 4. Enhance email validation 5. Improve login error messaging 6. Add "Optional" indicators to non-required fields

Quality Improvements: 7. Enforce minimum length for organization names 8. Correct content typos (testimonial, system message)

Addressing the High and Medium-High priority issues will significantly reduce user drop-off, frustration, and support requests. Resolving the Medium and Low priority items will enhance data quality, platform trust, and overall professional polish.

Recommended Next Steps: Address these issues in priority order, beginning with the critical authentication flow bugs (OTP Resend, Confirm Password) and the security-adjacent password policy update. A phased approach with quick wins on content fixes can demonstrate immediate responsiveness while larger validation framework improvements are developed.