Individual privacy issues in online rare disease communities: best practices and recommendations

P Priyanka, JD, CIPP/E; Justin Gay; Mukund Nori, PhD, MBA, CMPP

rareLife solutions, Norwalk, CT, USA

Introduction

- Although we all instinctively understand "individual privacy," it is not very well defined and can mean different things based on age, cultural background, education, etc[1-3]
  - These differences in understanding are exacerbated in the digital age, when access to personal information may also be a barrier[1]
- By definition, there are very few patients affected by any rare disease, and they are spread all over the world[4,5]
  - The rarity of these diseases makes it difficult for patients, caregivers, and health care professionals (HCPs) in any single geographic region to amass enough data to make informed decisions about treatment and management of the disease
- The COVID-19 pandemic has only magnified the existing problems
  - It was already difficult to separate high-quality, curated information from the ocean of noise
  - However, face-to-face discussions, especially at relevant medical or rare disease conferences, helped people assess for themselves the value of the available information
- There is an essential need to obtain and exchange critical information on rare diseases to be able to better treat and manage rare diseases among patients
- Therefore, it is natural in the digital age for patients, advocates, and caregivers (PACs) to establish and build their own disease-specific online communities[6]
  - In the absence of easily accessible, peer-reviewed publications, most of the information PACs obtain is from the internet, where there is little or no quality control[7]
  - Thus, high-quality, freely accessible, peer-reviewed medical literature, both in print and online, is necessary to provide the information essential to HCPs and PACs
- The onevoice platforms are designed to facilitate vibrant online communities for people impacted by or interested in specific rare diseases to access curated educational content and interact with each other in a safe environment
- It is incumbent on the owners and managers of online communities to ensure individual privacy
  - This is even more challenging for online communities for rare diseases because there are so few patients

Objective

- To identify and address individual privacy issues in online rare disease communities

Methods

- We conducted a privacy review of policies and practices on 5 active community platforms
- We evaluated the following parameters:
  - Registration requirements
  - Data retention
  - Ease of understanding of privacy
  - Safeguards
  - Compliance with the General Data Protection Regulation (GDPR) and the Children's Online Privacy Protection Act (COPPA)[8,9]
  - Other practices affecting individual privacy

Results

- As summarized in **Table 1**, many of the features and practices in effect on these platforms help protect individual privacy

Table 1. Summary of Privacy Features on Platforms Evaluated

Feature	Policy/practice	Privacy impact
Registration	Fields required: • Valid email address • Username (no restrictions) • ZIP code (if applicable) • Role in community	• Easy to use • Registrants are advised to have a username different from their name • Members have the option to keep their ZIP code hidden
Sharing of information	• Members can voluntarily share any personal information on the platform or externally to other social media	• Members are advised not to share personal identifiers; however, the decision is left to the member
Platform social wall	• Can be accessed only by registered members • Members can voluntarily share any personal information	• Nonmembers cannot access the social wall • Members are advised not to share personal identifiers; however, the decision is left to the member
Privacy policy	• Privacy policy stated in easy-to-understand language • Rollout of a layered step-by-step process to guide members on the privacy policy is in progress	• Compliant with current legislation and guidelines (GDPR, COPPA, etc) • Members can understand and proactively manage their privacy risk and exposure
User rights	• Users can exercise all rights under current domestic and international privacy laws • Users can withdraw permission for using their data • Team response without undue delay (usually within a few hours) to ensure compliance with privacy laws	• Compliant with current legislation and guidelines (GDPR, COPPA, etc) • Generates and maintains trust in the platform with respect to privacy
Cookies	• No advertising cookies • Cookies deleted at the end of each session	• Compliant with current legislation and guidelines (GDPR, COPPA, etc) • No individual user metrics are collected, ensuring individual privacy

Abbreviations: COPPA, Children's Online Privacy Protection Act; GDPR, General Data Protection Regulation.

- Registration (**Figure 1**)
  - The registration requirements are minimal and easy to provide
  - Registrants are able to have a username different from their actual name
  - Once registered, members have the option to keep their ZIP code hidden

Figure 1. Example of Registration Requirements on a onevoice Platform

- Privacy policy (**Figure 2**)
  - The privacy policy is easy to read and compliant with current legislation and guidelines
  - Members are empowered and encouraged to proactively manage their privacy risk and exposure
  - There is a privacy and security team available 24/7 to assist with any request regarding onevoice products and services

Figure 2. Example of Privacy Policy on a onevoice Platform

- Session cookies (**Figure 3**)
  - All platforms prohibit advertisement cookies
  - Session cookies are deleted at the end of each session
  - No individual user metrics are collected to ensure individual privacy

Figure 3. Example of Cookie Banner on a onevoice Platform

- There were also some additional actions being undertaken to proactively address potential systemic risks to privacy on these platforms (**Table 2**)

Table 2. Summary of Potential Risks and Solutions Being Enacted on Platforms

Potential privacy risk	Solutions enacted or in progress	Privacy impact
Overcollection of data	• Data retention policy under review and revision to incorporate data minimization principle	• Reduces risk of collecting unintended personal data • Data loss minimization in case of breach
User data anonymity	• Contact information of platform visitors is not recorded	• No information connecting visitors to platform statistics ensures user anonymity at the preregistration stage
Unauthorized data collection	• Users need to actively consent to their data being collected • Data are used only for indicated reasons	• Ensures informed consent from the users for the data being collected • Transparency regarding the purpose for which data are collected
Unauthorized data exchange	• Data collected are used only for indicated reasons • Data are not provided to anyone not authorized • Data are not sold	• Compliant with current legislation and guidelines (GDPR, COPPA, etc) • Maintaining data confidentiality protects users' rights
Jeopardy of identity disclosure	• Deployment of just-in-time notices to inform and guide users on using pseudonyms in progress	• A just-in-time notice to ensure transparency as required by Article 12 of the GDPR
Tracking	• No device tracking is used	• Compliant with current legislation and guidelines (GDPR, COPPA, etc)
Malware	• Alerting set up for potential attacks • Penetration testing performed periodically	• Proactively guard against identity theft and data breach

Abbreviations: COPPA, Children's Online Privacy Protection Act; GDPR, General Data Protection Regulation.

- A layered, step-by-step process in easy-to-understand language to explain the privacy policy is in development
- These platforms are pressure tested periodically to ensure that they maintain security
- Tracking (**Figure 4**)
  - Alerts are in place to identify potential attacks and proactively guard against data breach and identity theft
  - The platforms are tested periodically for penetrability to ensure security
  - These graphs represent that the onevoice platforms are healthy and not under attack by potential hackers or exploits
  - Any alert triggers troubleshooting to identify the cause
  - Suspected hackers are blocked, and other proprietary defensive measures are enacted

Figure 4. Graphical Representation of Security on a onevoice Platform
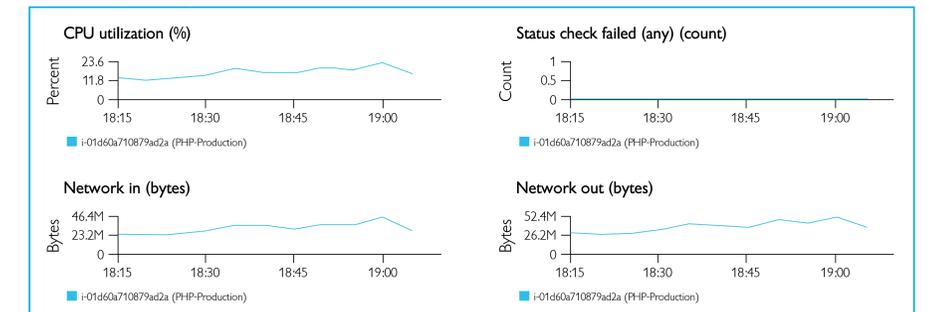
Limitations

- This evaluation was conducted only on the onevoice platforms; other sites were not included
- There are currently 5 active onevoice platforms
- The evaluation was led by an internal privacy officer

Discussion and conclusions

- Individual privacy, especially in the rare disease community, is difficult to maintain
  - Nevertheless, it is critical for the confidential and trusted exchange of personal information
- The onevoice online communities were designed to provide a safe and trusted source for patients, caregivers, and others interested in rare diseases to obtain curated information in the format of their preference and to interact with each other without loss of individual privacy
  - These platforms were also designed to ensure ease of access to educational information for anyone visiting the site
- To limit access and increase individual privacy, several features, such as interacting with others on the social wall, participating in polls and surveys, and exchanging information, are only available to those who are registered as members
- Although registration requirements are minimal, members are proactively guided on best practices to ensure their privacy
- These platforms are compliant with all current legislation and guidelines on privacy
- A vigilant site security process is in place to address new threats and issues as they come to light through internal review or recommendations from community members
- Ensuring individual privacy appears to be central to the onevoice platforms

References

1. Kelly G, McKenzie B. *J Med Internet Res*. 2002;4:e12.
2. Livingstone S, et al. EU Kids Online. Accessed September 9, 2021. http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf
3. Capurro R. *Ethics Inf Technol*. 2005;7:37-47.
4. US Food and Drug Administration. Rare diseases: common issues in drug development guidance for industry. Accessed April 11, 2019. https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM629579.pdf
5. Wakap SN, et al. *Eur J Hum Genet*. 2020;28:165-173.
6. Rose SL. *J Law Med Ethics*. 2013;40:680-687.
7. Pauer F, et al. *J Med Internet Res*. 2017;19:e23.
8. European Commission. General Data Protection Regulation. Accessed December 3, 2020. https://gdpr-info.eu/
9. Federal Trade Commission. 16 CFR Part 312, Children's Online Privacy Protection Rule; Final Rule. Accessed September 10, 2021. https://www.ftc.gov/system/files/2012-31341.pdf