Privacy Explanation Checklist

Assesses which actions are taken to enable users to understand how well their privacy is maintained by the program, that is, in order to enable users to determine whether and how to use it.

Sum items score range 0–8; Suggested interpretation: 0 = meets user privacy explanation checklist requirements.

No.	Item	Yes	N / A	No or can't tell
Terms of Use				
1	The system informs users of the data journey in detail so they understand all sources of data exposure (and risks if their device or app are not password-protected). This includes data stored on servers and on the device	0	0	1
2	The system notifies users how their personal identifiable information will be kept confidential and secured.	0	0	1
3	The system notifies users about how gathered data may be used (e.g., for commercial reasons).	0	0	1
4	For programs explicitly designed to be used by minors, the system includes a section requiring the approval/supervision of a legal guardian.	0	0	1
5	The system explicitly tunnels users through the terms of use (privacy/data wise, including items #1-#3, and #4 [if applicable]) before program utilization. In cases in which all other items are N/A, the system generally states that it does not collect any data, identifications, etc.	0	0	1
Systems with In-House Social Platforms				
6	The system enables users to keep identifiers private (and this is the default setting).	0	0	1
7	It is apparent when information will be seen by other users/members even if data do not contain identifiers (e.g., when they are in a particular zone where data are not kept private).	0	0	1
8	The system warns users about providing private identifiable information (e.g., name, health information, home address) to other users on the platform.	0	0	1

Notes: Pay attention to the permissions apps are given when the user is downloading them (in terms of data they access);
Among others, identifiers include the recording of device ID (but not stating how device_id will be de-identified); email address; Facebook account for authentication; phone number; recording of a username that is not automatically directed to be fictional; and any place in which open notes can be written within the program (in which identifiers can be documented).
If not stated otherwise, it should be assumed that programs gather utilization data to their servers. Utilization data gathered from health programs/apps should be considered personal health information if found on a device (which is automatically identified with the owner) or on servers (only if identifier is also accessed/recorded).

