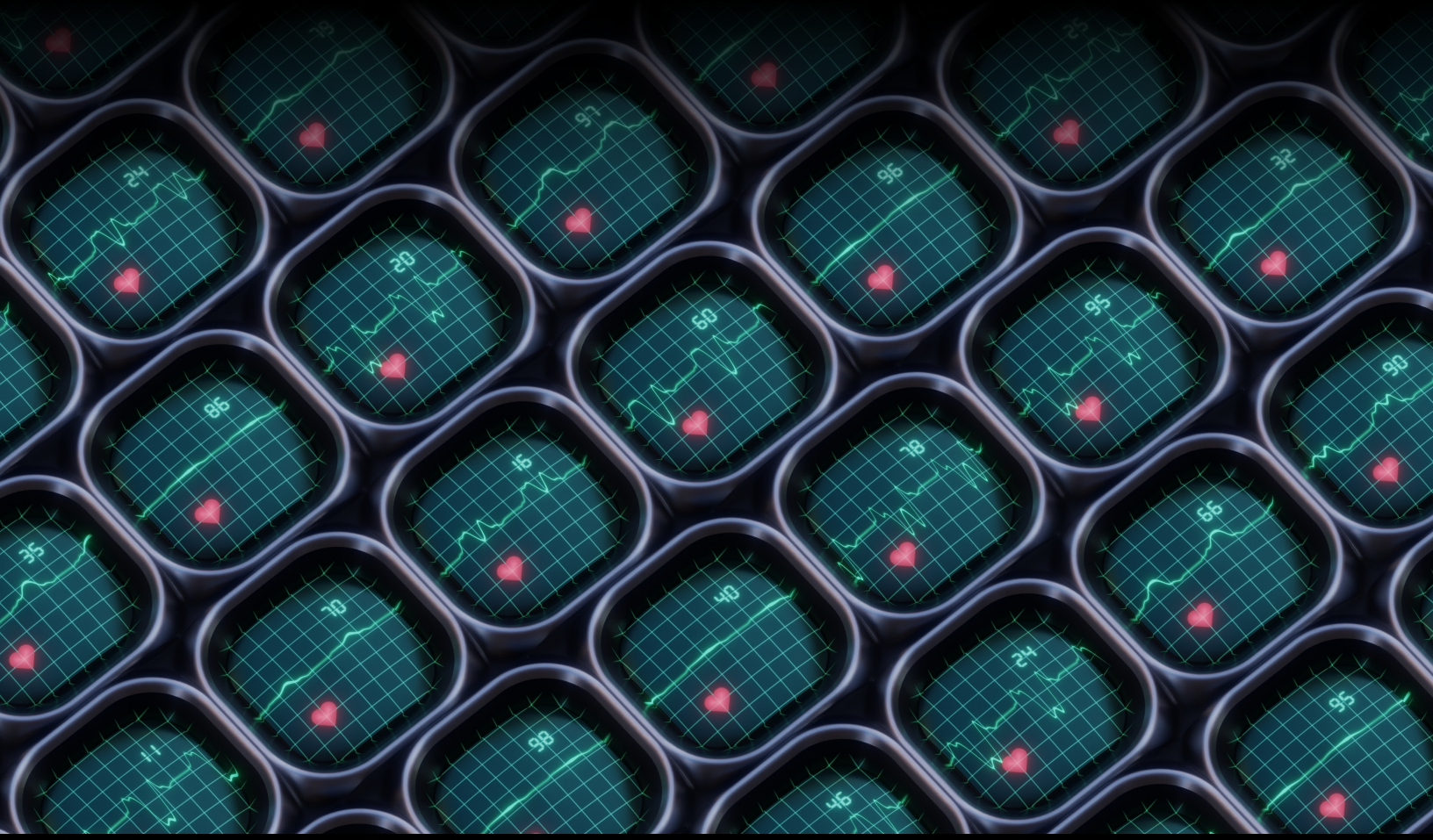
UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY



CLTC WHITE PAPER SERIES

A Template for Voluntary Corporate Reporting on Data Governance, Cybersecurity, and AI

DESIGNED FOR THE MOBILE HEALTH MARKET

JORDAN FAMULARO

Cover photo by Mingwei Lim on Unsplash

CLTC WHITE PAPER SERIES

A Template for Voluntary Corporate Reporting on Data Governance, Cybersecurity, and AI

DESIGNED FOR THE MOBILE HEALTH MARKET

JORDAN FAMULARO

August 2023

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Capital markets are shifting the norms for corporate disclosure on technology topics, particularly data governance, cybersecurity, and artificial intelligence. This paper presents a template for such disclosure in the mobile health market, designed to guide more consistent reporting by companies and to propel better information for investors concerned about financial materiality, human rights, and equity.

Partly driven by demand from investors, many companies are developing new approaches to explaining their handling of data governance, cybersecurity, and artificial intelligence (AI) through corporate disclosure. Firms are progressively centralizing information on technology topics in reports on their websites under headings like Investor Relations, Corporate Responsibility, ESG (Environmental, Social, Governance), and Sustainability. Yet without solid norms about what this reporting should look like, there is no recognizable consistency across companies or comparability over time, raising doubts about the effectiveness of the information for augmenting investor decision-making and catalyzing better corporate practices.

A streamlined and systematic reporting template is needed to guide companies and investors toward a clearer set of norms about disclosures on data governance, cybersecurity, and AI. This study seeks to meet these corporate and investor needs by focusing on reporting by companies through a pilot study designed for the mobile health market, which provides healthcare solutions through technologies such as sensors, smartphones, networks, and analytics, and is estimated to reach $310 billion by 2027.[1] The study's target companies have maturity levels on a spectrum from Series C (high-growth startups with established market presence) to public (mature companies with publicly traded shares).

We conducted a Delphi study (a structured consensus-building process) and interviews with a panel of 20 experts from eight countries to define a set of critical disclosures on cutting-edge technology topics for companies in the mobile health market. The goals were to select and systematize the most critical disclosure recommendations from authoritative sources in the private and non-profit sectors, organize them into a user-friendly reporting template, and aid reporting practice by appending commentary and definition updates.

1 BioSpace, "Mobile Health Market Growth 2022–2030: Rapid Digitalization in The Healthcare Sector," (June 14, 2022), https://www.biospace.com/article/mobile-health-market-growth-2022-2030-rapid-digitalization-in-the-healthcare-sector/.

From our results, we produced a reporting template to guide voluntary disclosure by companies in the mobile health market with a systematic set of 26 prompts, organized by theme (data governance, cybersecurity, and AI). Instructions and references are included. The template is available at https://cltc.berkeley.edu/publication/corporate-reporting-template. Though mobile health is a specific market with distinct digital responsibility disclosure needs, this work could also inform adaptations for different markets, verticals, and industries.

This guide orients readers to the template, describes the development process, and gives detailed disclosure guidance.

Introduction

"I'm a big believer in transparency. And transparency will allow us to understand how every company moves forward in a transition. We are not dictating how a company goes forward, but we are asking each company to be transparent and tell us [its] pathway. . . . Through that transparency I do believe we move faster as a society."

—Larry Fink, CEO of BlackRock

Larry Fink was speaking about climate disclosure when he made the statement above in 2021, but a 2023 version of this talk could have just as easily been concerned with digital transition and the pressure it creates for companies to explain their risks and opportunities publicly.

How might companies' management of digital technology become a mainstay of corporate responsibility, alongside areas like environmental practices and workplace safety? The University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC) has been exploring this question with a dual focus on how companies communicate aspects of digital responsibility to investors, and how norms for corporate disclosure evolve.

Our focus on corporate disclosure has two notable benefits as a study of communication systems. First, corporate disclosure is a critical part of an ongoing paradigm shift about business responsibility. Companies have in recent years consolidated reporting about their environmental, social, and governance (ESG) performance, largely as a result of expectations from capital markets, regulators, advocacy organizations, consumers, and other stakeholders. For these actors, pressing for improved corporate disclosure is a key part of *field building*, or influencing the environments in which companies are embedded through changes in norms, conventions, and standards.[2] Modes of field building can range from establishing

In this research, "corporate disclosure" is a broad term referring to both voluntary and statutory communication by which companies report financial and/or nonfinancial information to their external stakeholders.

2 For a recent review of field building, see Emilio Marti, Martin Fuchs, Mark R. DesJardine, Rieneke Slager, and Jean-Pascal Gond, "The Impact of Sustainable Investing: A Multidisciplinary Review," *Journal of Management Studies*, early view preprint (June 2, 2023), https://doi.org/10.1111/joms.12957.

voluntary reporting standards to stigmatizing certain business activities. This is far from "transparency for transparency's sake," an untested assumption that daylight must be a solution to problems stemming from information asymmetry among parties, such as those related to business responsibility.

The second advantage of focusing on corporate disclosure is that the evidence is trackable. In an era when plentiful information can be known about a given business through search engines and digital media, companies are adding their official voice through more channels than ever. Public companies in particular are centralizing information about technology issues that stakeholders care about in reports posted on their websites under headings like Investor Relations, Corporate Responsibility, ESG, and Sustainability.

OBJECTIVES

This paper shares the results of a distinctive consensus-building and interview process conducted in spring 2023. The purpose of the research was to illuminate ties between corporate disclosure and digital responsibility, and to produce a tool that offers some reporting guideposts for companies, investors, and their observers.

Our first aim is to offer a systematic, empirically tested, user-friendly template that guides voluntary disclosure by companies on data governance, cybersecurity, and AI, and that informs investors' expectations for such reporting.

Our second aim is to provide a groundwork for future efforts by the private, public, and non-profit sectors to clarify expectations for corporate disclosure on data governance, cybersecurity, AI, and related topics.

SCOPE

This is a pilot study focused on a specific market: consumer-facing mobile health (see sidebar). This market comprises firms that provide healthcare solutions through mobile technologies, such as sensors, wearables, monitors, and smartphones, that are enhanced by networks and analytics. Market segments include telemedicine, remote patient monitoring, personalized health trackers, fitness apps, behavior modification tools, genomic testing, personalized testing, and biometric monitoring wearables. The market includes (but is broader than) the

field of digital therapeutics, the delivery of medical interventions directly to patients through evidence-based, clinically evaluated software to treat, manage, and prevent diseases and disorders.

The global mobile health market is estimated to reach $310 billion by 2027, an increase from $52 billion in 2021.[3] As the market continues to grow, business-to-consumer (B2C) mobile health companies represent a new frontier in corporate reporting because they combine the leading edge of corporate transparency concerns about technology with highly sensitive concerns about health, human rights, and equity that could also impact companies' financial performance. Over decades, observers have pointed out gaps between policy protections for health-related data and the advancement of business systems that ingest, analyze, and share that data.[4] B2C mobile health companies present a rich set of issues along three dimensions that are important to investors: financial materiality, human rights, and equity.

PLAYERS IN B2C MOBILE HEALTH

- Companies that make medical devices and apps, like **Philips** and **Omron**
- Tech giants that offer fitness wearables, like **Alphabet** [Fitbit] and **Amazon** [Halo]
- Wellness companies that offer mobile apps, like **WW International** [formerly Weight Watchers International]
- Consumer tech companies that make health and wellness devices used in the home or on the go, like **Apple**
- Pharmaceutical companies that are expanding their therapeutic expertise to emerging technologies, like **Johnson & Johnson**
- Telecoms that offer platforms for mobile health, like **AT&T**
- Drug retailers that incorporate consumer healthtech devices into their loyalty programs, like **Walgreens**
- Apparel companies that embed apps, devices, and platforms into their digital fitness programs, like **Nike**
- Interactive insurance companies that offer health and wellness tech to collect consumer data in exchange for discounts and perks, like **John Hancock**

- **Financial materiality:** Mobile health companies face a number of risks that may be financially material in the ways that they manage data, AI, and cybersecurity. These include

3 BioSpace, "Mobile Health Market Growth 2022–2030: Rapid Digitalization in The Healthcare Sector," (June 14, 2022), https://www.biospace.com/article/mobile-health-market-growth-2022-2030-rapid-digitalization-in-the-healthcare-sector/.

4 For example, see Lisa Parker et al., "The 'Hot Potato' of Mental Health App Regulation: A Critical Case Study of the Australian Policy Arena," *International Journal of Health Policy and Management* 8, no. 3 (2019): 168–76, https://doi.org/10.15171/ijhpm.2018.117; United Kingdom Information Commissioner's Office, "Tech Horizons Report," (December 2022), https://ico.org.uk/media/about-the-ico/documents/4023338/ico-future-tech-report-20221214.pdf; and Müge Fazlioglu, "Filling the Void? The 2023 State Privacy Laws and Consumer Health Data," International Association of Privacy Professionals (March 28, 2023), https://iapp.org/news/a/filling-the-void-the-2023-state-privacy-laws-and-consumer-health-data/.

strategic, regulatory, operational, counterparty, cybersecurity, reputation, and intellectual property exploitation risks. In relation to financially material risks in corporate data governance, AI, and cybersecurity, companies will need to vigilantly keep up with changing societal expectations and legal requirements regarding corporate financial and ESG reporting.

» *Example:* Netherlands-based health technology company Koninklijke Philips NV (Royal Philips) describes technology-related and financially material risks in its 2022 annual report. For example, the report states that "failures in internal controls or other issues with respect to Philips' public disclosures, including disclosures with respect to cybersecurity risks and incidents, could create market uncertainty regarding the reliability of the information (including financial data) presented. This could have a negative impact on the price of Philips securities."[5]

- **Human rights:** Investors have shared concerns with prominent "Big Tech" companies about human rights and the potential financial impacts of user-generated content, targeted advertising, and privacy breaches, among other topics.[6] Mobile health companies' business practices have been implicated in similar issues.

  » *Example*: Ovia Health, a subsidiary of Labcorp, has reportedly collected billions of data points on women's health with its pregnancy-tracking app, Ovia. A 2019 *Washington Post* investigation by reporter Drew Harwell found that the company profits from targeted advertising and from selling aggregated data to employers and insurance companies.[7] Harwell collected concerns about potential harms from privacy experts and a user of the app whose data was made available to her employer in aggregate with the data of other users.

- **Equity:** On one hand, mobile health products and services create the potential for more accessible, personalized, and frequent health interventions that address inequities in care, illness prevention, and research. On the other hand, the collection of data managed by mo-

5 Koninklijke Philips NV (Royal Philips), Amendment No. 1 to Form 20-F/A, Annual Report, (February 24, 2023), 9.5, Financial Risks, available at https://www.sec.gov/edgar/browse/?CIK=0000313216&owner=include.

6 Investor Alliance for Human Rights, "Through a Series of Shareholder Proposals at Alphabet, Amazon and Meta Investors Underscore Digital and Human Rights Risks in Tech Sector," (January 31, 2023), https://investorsforhumanrights.org/news/through-series-shareholder-proposals-alphabet-amazon-and-meta-investors-underscore-digital-and.

7 Drew Harwell, "Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?" *Washington Post* (April 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/.

bile health apps, devices, and platforms raises questions about governance, AI bias, security, privacy, inclusion, and autonomy specific to systematically excluded groups, all of which could impact a company's financial performance.

- *Example:* Sensors used in Apple Watch's pulse oximeter device are less accurate when worn by someone with darker skin, which has led to a class-action lawsuit against Apple.[8]

This project builds on our prior research, which found that investors in particular are bringing focus on digital responsibility disclosure to sectors beyond "Big Tech," such as healthcare, pharmaceuticals, and financial services.[9] Data governance, cybersecurity, and AI are concerns that infuse every sector and are on the rise in engagements regarding ESG and other nonfinancial disclosures.

THE CHALLENGE

A driving assumption in this research is that mature companies face or will soon face "reporting fatigue"[10] as they are asked to respond to pro-forma questions on a range of ESG issues, whether for investors, ratings agencies, private research firms, or advocacy organizations. The proliferation of voluntary reporting recommendations on data governance, cybersecurity, and AI by private and non-profit actors has contributed to or will soon contribute to information dilution, unclear expectations, and resource exhaustion.

Our prior research found that corporate reporting fatigue is a significant impediment to disclosure at the firm level that also limits agreement on best practices at the industry level.[11] More than an implementation challenge, reporting requirements give rise to a number of capacity and oversight questions. As Stephen Pitt-Walker of Optima Board Services Group and the Governance Institute of Australia said: "Who's going to do it? Who's going to manage it?

8 Emma Woollacott, "Apple Sued Over 'Racial Bias' Of Apple Watch," *Forbes* (December 29, 2022), https://www.forbes.com/sites/emmawoollacott/2022/12/29/apple-sued-over-racial-bias-of-apple-watch/.

9 Jordan Famularo, "Future Directions in Corporate Disclosure on Digital Responsibility," *CLTC White Paper Series* (June 2023), 26–27, https://cltc.berkeley.edu/publication/future-directions-in-corporate-disclosure-on-digital-responsibility/.

10 Silvia Pavoni, "Proliferation of Demands Risks 'Sustainability Reporting Fatigue,'" *Financial Times* (May 11, 2020), https://www.ft.com/content/9692adda-5d73-11ea-ac5e-df00963c20e6.

11 Jordan Famularo, "Future Directions in Corporate Disclosure on Digital Responsibility," *CLTC White Paper Series* (June 2023), 21–22, https://cltc.berkeley.edu/publication/future-directions-in-corporate-disclosure-on-digital-responsibility/.

What does it mean for audit capacity? What does it mean for the audit committee? What does it mean for the risk committee as well? Because they are stakeholders to that information, too."

A systematic reporting template is needed to guide companies and investors toward a clearer set of norms about disclosures on data governance, cybersecurity, and AI. While public companies are already under significant stakeholder pressure to make these disclosures, growth companies with IPO ambitions should be preparing for similar demands. This study seeks to meet these corporate and investor needs.

OUTPUTS

This study produced two main outputs:

1. This **guide**, which describes our methodology and orients readers to the template (see below) while giving detailed guidance for using the template.

2. A **reporting template** to guide disclosure by companies in the mobile health market and inform investor expectations with a systematic set of 26 prompts, organized by theme (data governance, cybersecurity, and AI).
   - Instructions and references are included.
   - The template is available at https://cltc.berkeley.edu/publication/corporate-reporting-template.
   - The template is intended for Series C to public companies and investors or potential investors in companies that provide mobile health products or services.

CLTC anticipates that the project outputs will be helpful to the following stakeholders:

- **Investors** seeking to understand financially material risks, human rights risks, and salient equity issues across the B2C mobile health market;
- **Sustainability, corporate responsibility, and ESG practitioners** at companies in the B2C mobile health market seeking to understand stakeholder priorities regarding disclosure;
- **Executive management and boards** reviewing expectations in the voluntary reporting landscape for B2C mobile health companies and/or disclosures on data governance, AI governance, or cybersecurity;

- **Civil society organizations** engaging companies and governments on priority human rights and equity issues in the B2C mobile health market;
- **Regulators and policy-makers** seeking to explore interventions in corporate reporting regarding data governance, AI governance, cybersecurity, and/or mobile health;
- **Human rights assessors** seeking to help companies conduct human rights due diligence;
- **Standard-setters** exploring development of reporting guidelines relevant to data governance, AI governance, cybersecurity, and/or mobile health companies; and
- **Consultants and advisors** providing services to any of the above.

Template Development

OVERVIEW

This reporting template was developed through empirical data collection by means of surveys and interviews, which were used to define a set of critical disclosures on data governance, cybersecurity, and AI for companies in the mobile health market. The research had a two-step structure:

1. Perform a Delphi technique (see sidebar) with a panel of 20 experts to select and systematize the most critical disclosure recommendations from authoritative sources in the private and non-profit sectors. This process was carried out through a series of three iterated surveys.
2. Conduct post-survey interviews to inform the composition of guidance for each item in the final set of disclosure recommendations identified in step 1.

For a detailed explanation of the study methodology, see Appendix A.

WHAT IS A DELPHI TECHNIQUE?

A Delphi technique is a method for achieving convergence of opinion concerning real-world knowledge solicited from experts. It involves a group communication process that is commonly used for conducting detailed examinations and discussions of a specific issue for the purpose of forecasting, goal setting, or policy investigation. The group communication process has some characteristic features, three of which were key to this research:

1. The researcher deploys multiple iterations of surveys or questionnaires;
2. The researcher provides confidentiality to respondents; and
3. The researcher administers controlled feedback at intermediate points in the study.

The objective here was to correlate informed judgments spanning a wide range of disciplines about which disclosures should be made.

RESULTS

The study's central finding was that 20 subject-matter experts from eight countries identified a set of 26 critical disclosures on data governance, cybersecurity, and AI for mature companies in the mobile health market. The survey series generated the set of disclosures, which form the basis for the reporting template, contextualized with observations from eight interviews with nine participants.

The 26 disclosure items consist of 12 data governance (D) disclosures, nine cybersecurity (C) disclosures, and five AI (A) disclosures. For ease of reference, we grouped them by theme and assigned each an identifier (D1–D12, C1–C9, and A1–A5). A list of the disclosures — organized by theme, topic, and in some cases subtopic — is as follows:

Data Governance

Policy / Commitments

D1. Disclose a privacy and/or data protection policy that covers the organization's entire operations, including third parties.

Practices

Data collection

D2. Disclose each type of user information the organization collects.

D3. Disclose the full range of purposes for which the organization collects data (including core business and additional commercialization purposes).

D4. Disclose how the organization collects user information from third parties.

D5. Disclose whether the organization collects user information from third parties by tracking people across the web using cookies, widgets, or other tracking tools embedded on third-party websites.

Inference

D6. Disclose the full range of purposes for which the organization infers data (including core business and additional commercialization purposes).

Data sharing

D7. Disclose each type of user information the organization shares.

D8. Disclose the full range of purposes for which the organization shares data (including for its core business and additional commercialization purposes).

Data retention

D9. Disclose the duration of time for which the organization retains user information.

D10. Disclose the full range of purposes for which the organization retains data (including core business and additional commercialization purposes).

Third-party requests to share user information

D11. Disclose the process for responding to third-party requests (by both government and private parties) to share user information.

Targeted advertising

D12. Disclose whether the organization conducts robust, systematic risk assessment for targeted advertising policies and practices.

Cybersecurity

Personnel/resources

C1. Disclose whether the organization has a cyber and/or information security team.

Incidents & response

C2. Disclose whether the organization has established an incident management plan that includes plans for disaster recovery and business continuity.
C3. Disclose material cybersecurity incidents.
C4. Disclose the number of users affected by data breaches.
C5. Disclose the percentage of data breaches involving personal information.
C6. Disclose the percentage of data breaches involving consumer health data.
C7. Disclose the number of breaches of customer data.

Resilience

C8. Disclose how the organization addresses security vulnerabilities when they are discovered.
C9. Disclose a description of policies and practices used to secure customers' consumer health data and personal information.

AI

Policy

A1. Disclose the organization's policy for AI governance.

Practices

A2. Disclose the range of purposes for which algorithmic systems are used.
A3. Disclose how the organization takes action to eliminate racial, gender, and other biases in algorithms.
A4. Disclose whether the organization conducts human rights due diligence to identify and mitigate the potential risks of algorithmic systems.
A5. Disclose whether the organization conducts robust, systematic risk assessment for algorithmic systems.

SOURCES

Study participants rated the criticality of 87 distinct disclosures in the survey series. The majority (73/87) of disclosures tested in the surveys were adapted from publications by eight organizations involved in the development of corporate digital responsibility and transparency

norms. Two of these are independent standard-setting organizations, three are non-profit advocacy organizations, one is an institutional investor, and two are multistakeholder organizations. Listed below are the eight sources, preceded by the corresponding abbreviation used in this report and the accompanying template.

EOS	EOS at Federated Hermes, EOS Digital Rights Principles (April 2022)[12]
Equal AI	Equal AI, Checklist to Identify Bias in AI (2020)[13]
GRI	Global Reporting Initiative, Standards (2016–22)[14]
PRI	U.N. Principles for Responsible Investment, "Stepping Up Governance on Cyber Security: What is Corporate Disclosure Telling Investors?" (2018)[15]
RDR	Ranking Digital Rights, Corporate Accountability Index (2020)[16]
SASB	Sustainability Accounting Standards Board,[17] Drug Retailers Sustainability Accounting Standard (2018), Health Care Delivery Sustainability Accounting Standard (2018), and Internet Media & Services Sustainability Accounting Standard (2018)
WBA	World Benchmarking Allliance, Digital Inclusion Benchmark (2020)[18]
WEF	World Economic Forum, "Measuring Stakeholder Capitalism: Towards Common Metrics and Consistent Reporting of Sustainable Value Creation" (2020)[19]

Legend:
Institutional investor | Multistakeholder organization | Non-profit | Independent standard-setter

EXPERIMENTAL DISCLOSURES

A minority (14/87) of tested disclosures were experimental, created by the researcher. For a list of experimental disclosures and a rationale for their use, see Appendix C.

12 https://www.hermes-investment.com/uploads/2022/04/5a8aadeb037fb131b1889c3f6b1a85aa/eos-corporate-digital-rights-principles-04-2022.pdf
13 https://www.equalai.org/assets/docs/EqualAI_Checklist_for_Identifying_Bias_in_AI.pdf
14 https://www.globalreporting.org/standards/download-the-standards/
15 https://www.unpri.org/governance-issues/stepping-up-governance-on-cyber-security/3452.article
16 https://rankingdigitalrights.org/index2020/methodology
17 SASB Standards are available at https://www.sasb.org/standards/download/
18 https://assets.worldbenchmarkingalliance.org/app/uploads/2020/09/Digital-Inclusion-Benchmark_Methodology-report_2020.pdf
19 https://www.weforum.org/reports/measuring-stakeholder-capitalism-towards-common-metrics-and-consistent-reporting-of-sustainable-value-creation/

How to Use the Template

OVERVIEW

The reporting template is intended to supply investors and companies involved in the mobile health market with a framework for monitoring, disclosing, and evaluating risks and opportunities related to data governance, cybersecurity, and AI.[20] The template is designed for reporting by companies on a spectrum from Series C (high-growth startup with established market presence) to public (mature company with publicly traded shares).

We recognize that companies may be prevented from disclosing information by law, or may choose not to disclose information because they wish to protect attorney-client privilege or trade secrets. At the same time, there is mounting pressure from external stakeholders, particularly investors, to reduce information asymmetry with regard to a range of environmental, social, and governance topics, including data governance, cybersecurity, and AI. Our research provides some guideposts toward meeting this need.

The template is built to meet the following objectives:

For companies:

- Report companies' risks and opportunities related to data governance, cybersecurity, and AI to investors and other stakeholders.
- Calibrate operations and disclosures in line with concerns about financial materiality, human rights, and equity found in stakeholder perspectives.
- Showcase responsible digital technology governance through disclosure of information about policies, practices, resources, and resilience.

For investors:

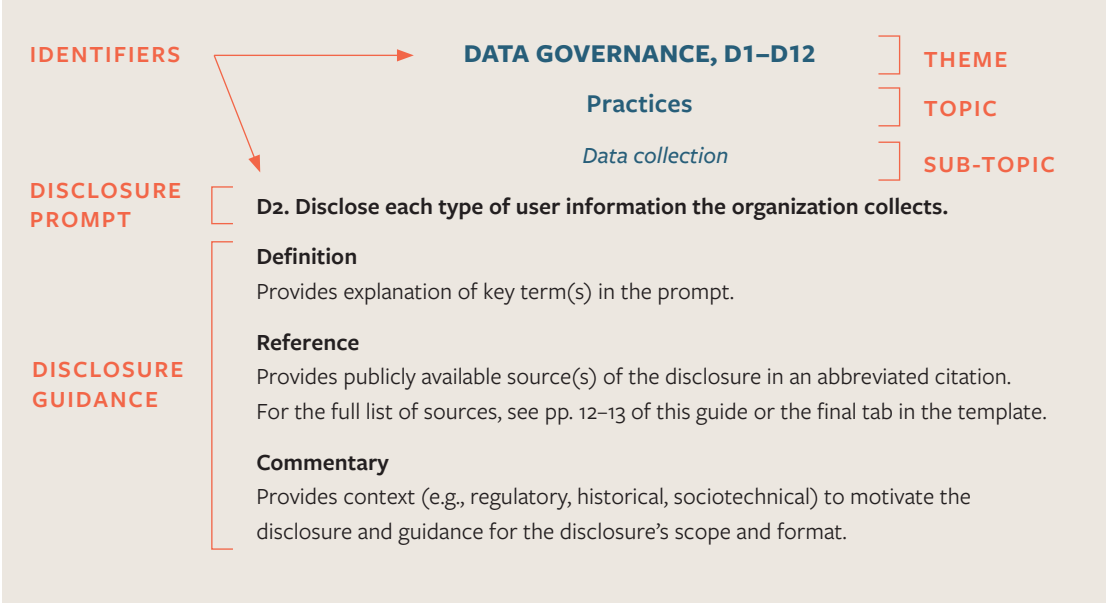
- Provide information about data governance, cybersecurity, and AI risks and opportunities relevant to financial materiality, human rights, and equity.
- Boost consistent reporting for companies involved in the mobile health market for comparability across firms.
- Propel disclosure of information that can lead to more effective dialogue and engagement between companies and investors.

20 The information contained in this document and accompanying framework is informational only and not intended to be advice for investment, legal, tax, or other purposes. Its intended purpose is to be auxiliary, not a determinant for decision-making.

INSTRUCTIONS

The template, which is in the form of a spreadsheet available at https://cltc.berkeley.edu/publication/corporate-reporting-template, contains an Instructions tab that explains where information inputs are needed. Throughout the spreadsheet, references point the user to specific parts of the Detailed Disclosure Guidance in this report (see the next section).

Model



Detailed Disclosure Guidance

DATA GOVERNANCE, D1–D12

Policy/Commitments

D1. Disclose a privacy and/or data protection policy that covers the organization's entire operations, including third parties.

Reference
PRI

Commentary
Good practice for this disclosure, according to U.N. Principles for Responsible Investment (PRI), includes a policy that "covers all company operations," including third parties.[21] Of relevance to investors, the management of data by third parties should be a priority, especially when storage, transmission, and handling of sensitive data is outside direct control of the company in question. Companies should disclose, and investors should want to know, whether the policy applies only to a specific website, a particular operation, or entire operations. Companies without an appropriately drafted policy in place risk regulatory fines, which can be substantial and even fatal to the business, according to our interview with Shannon Yavorksy, a partner at law firm Orrick Herrington & Sutcliffe LLP. The European Union's General Data Protection Regulation (GDPR) provides authority for imposing fines of up to 20 million Euros or 4 percent of the business's total annual worldwide revenues, whichever is higher.[22]

Practices

Data collection

D2. Disclose each type of user information the organization collects.

Definition
User. Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.[23]

Reference
SASB Drug Retailers Sustainability Accounting Standard (at HC-DR-230a.1, 2);
RDR (at P3)

21 U.N. Principles for Responsible Investment, "Stepping Up Governance on Cyber Security: What is Corporate Disclosure Telling Investors?" (2018), 8, https://www.unpri.org/governance-issues/stepping-up-governance-on-cyber-security/3452.article.

22 European Commission, "What If My Company/Organization Fails to Comply with the Data Protection Rules?" accessed June 10, 2023, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en.

23 Compare the definition of user at Global Network Initiative, "The GNI Principles: Annex A: Definitions," accessed June 15, 2023, https://globalnetworkinitiative.org/gni-principles/.

Commentary

Types of user information collected by market actors in mobile health — such as information about reproductive health, chronic conditions, and precise geolocation — have in recent years attracted attention from regulators, the media, and the public. For example, the U.S. Federal Trade Commission (FTC) filed a complaint against Kochava, a data broker, alleging that it acquired consumers' precise geolocation data, and then marketed it so that clients could track individuals' movements to and from sensitive locations, potentially including women's reproductive health clinics.[24]

Using this template, reporting organizations aligning with instructions in SASB standards may discuss which data or types of data are collected without consent of an individual, which data requires opt-in consent, and which requires opt-out action from the individual.

D3. Disclose the full range of purposes for which the organization collects data (including core business and additional commercialization purposes).

Reference

EOS;
RDR (at P5)

Commentary

Collecting sensitive data in a mobile health context for purposes of commercialization, particularly for targeted advertising, poses regulatory and reputational risk. Although the data brokerage industry incentivizes the collection of personal information for sharing and selling, there is growing awareness among citizens, regulators, researchers, and the media that these practices are not appropriate for some health-related contexts. The U.S. Federal Trade Commission's proposed order to settle charges with online counseling service BetterHelp exemplifies regulators' keen attention to privacy in consumer health settings. The order, which is pending as of this writing, bans BetterHelp from sharing individuals' health data, including sensitive information about mental health, for advertising and requires the company to pay a $7.8 million fine. The FTC's complaint alleges that BetterHelp shared its collection of sensitive data from users with third parties such as Facebook and Snapchat for advertising purposes after promising to keep such data private.[25]

D4. Disclose how the organization collects user information from third parties.

Definition

User. See the definition at D2.

Reference

RDR (at P9)

24 U.S. Federal Trade Commission, "FTC v Kochava, Inc.," last updated August 29, 2022, https://www.ftc.gov/legal-library/browse/cases-proceedings/ftc-v-kochava-inc.

25 U.S. Federal Trade Commission, "FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising," (March 2, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook.

Commentary

This disclosure helps investors, customers, and other stakeholders understand the company's interaction with tracking infrastructures and business tools, such as pixels and social plugins, that silently collect users' data as they navigate the internet and use applications. A major driver of the sharing and sale of data between organizations is the market for data enhancement, a practice of appending data from third-party sources to data obtained directly from consumers.[26] Consumers, advocates, and policymakers are concerned about the granular dossiers on individuals compiled by companies, which can be used to sort opportunities for those people and influence internet users' behavior through market nudges, such as predictions about how they will respond to advertising. From a human rights perspective, tracking infrastructure and its supporting tools give rise to concerns about how automated filtering of opportunities could lead to discrimination[27] and how market nudges may threaten personal autonomy.[28]

D5. Disclose whether the organization collects user information from third parties by tracking people across the web using cookies, widgets, or other tracking tools embedded on third-party websites.

Definition

User. See the definition at D2.

Reference

RDR (at P9)

Commentary

Companies that make this disclosure give an indication of their participation in third-party tracking networks. Third-party tracking, which allows companies to identify users and track their behavior across multiple digital services on desktop and mobile, supports internet-based advertising but has become widely perceived as privacy-invasive in recent years.[29] Internet and app ecosystems are often designed for maximum data collection, which is boosted by various tracking technologies. On the Web, trackers can log information about what users search, click, and type. On mobile, identifying codes — such as device and advertising identifiers — can track users across apps. In the wake of privacy concerns with such trackers, technologists have begun to replace advertising tools that rely on tracking people across the Web and mobile. However, third-party tracking is still ingrained in the consumer internet, which has recently led regulators such as the U.S. Federal Trade Commission and Department of Health and Human Services to investigate how mobile health companies market their services online, and to impose penalties for misconduct.[30] In response to this regulator activity, several organizations, including Monument, a telehealth company focused on alcoholism recovery, notified customers that they have disabled use of

26 Joel Stein, "Data Mining: How Companies Now Know Everything About You," *Time Magazine* (March 10, 2011), http://content.time.com/time/magazine/article/0,9171,2058205,00.html.

27 Frederik Zuiderveen Borgesius, "Discrimination, Artificial Intelligence, and Algorithmic Decision-Making," Council of Europe Directorate General of Democracy (Strasbourg, 2018), https://www.coe.int/en/web/artificial-intelligence/-/news-of-the-european-commission-against-racism-and-intolerance-ecri-.

28 Viktor Ivanković and Bart Engelen, "Market Nudges and Autonomy," *Economics & Philosophy*, First View (2022): 1–28, https://doi.org/10.1017/S0266267122000347.

29 Lily Hay Newman, "Health Sites Let Ads Track Visitors Without Telling Them," *Wired* (February 6, 2022), https://www.wired.com/story/health-site-ad-tracking/; Brian X. Chen and Daisuke Wakabayashi, "You're Still Being Tracked on the Internet, Just in a Different Way," *New York Times* (April 6, 2022), https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html.

30 Ruth Reader, "'Shut It Off Immediately': The Health Industry Responds to Data Privacy Crackdown," *Politico* (April 17, 2023), https://www.politico.com/news/2023/04/17/health-industry-data-privacy-00092447.

third-party tracking technologies and filed a data breach notification with the appropriate government authorities.[31]

Inference

D6. Disclose the full range of purposes for which the organization infers data (including core business and additional commercialization purposes).

Reference
EOS;
RDR (at P5)

Commentary
Data analytics in mobile health contexts can produce inferences about individuals' spending preferences, risk of illness, life expectancy, lifestyle choices, mood disorder, chance of relapse, and many other factors.[32] Inferences are one of the key mechanisms by which information becomes valuable to businesses, yet their source and substance are virtually invisible to other parties. In the U.S. reproductive rights context, after the overturning of *Roe v. Wade*, there is concern that inferences about pregnancy or intentions to end a pregnancy are in the hands of companies, and that they could opt to share this information with law enforcement.[33] One interviewee in our study noted that inference from mobile health-related data can generate "deeply unethical, deeply unfair" outcomes, sometimes based on inaccurate data, which make transparency and the availability of remedy more important. By asking for *purposes* of inferences rather than what specifically the inferences are, our template allows companies discretion to condense their answers into what is useful for their stakeholders, depending on their specific business context. The intention is to accommodate companies that depend heavily on inferences.

Data sharing

D7. Disclose each type of user information the organization shares.

Definition
User. See the definition at D2.

Reference
SASB Drug Retailers Sustainability Accounting Standard (at HC-DR-230a.1, 2);
RDR (at P4)

Commentary
Data sharing is rampant in the mobile health market, particularly through apps. A 2021 analysis of 20,991 mobile health apps found that more than 87 percent of data collection practices were carried out on

31 California Office of the Attorney General, Submitted Breach Notification Sample [Monument] (March 28, 2023), https://oag.ca.gov/system/files/Monument%20-%20Sample%20Notification%20Letter%204888-3653-0266%20v.2.pdf.

32 G. Malgieri and G. Comandé, "Sensitive-by-distance: Quasi-health Data in the Algorithmic Era," *Information & Communications Technology Law* 26, no. 3 (2017): 229–49.

33 The threat is not just hypothetical. See Kevin Collier and Minyvonne Burke, "Facebook Turned Over Chat Messages between Mother and Daughter Now Charged Over Abortion," *NBC News* (August 9, 2022), https://www.nbcnews.com/tech/tech-news/facebook-turned-chat-messages-mother-daughter-now-charged-abortion-rcna42185.

behalf of third-party services.[34] By asking for the *types* of user information that the organization shares, our template allows companies discretion to provide either a granular list or a summary. The intention is to accommodate companies with large numbers of data sharing partners and arrangements, which may number in the hundreds or more. In one interview, Chris McClean, Global Lead for Digital Ethics at IT services and advisory firm Avanade, reminded us that data sharing practices can change frequently and may outpace the rate of disclosure. This gives rise to a need for some companies to disclose a summary of types of user information they share as part of a broader discussion of their data sharing framework — for example, what data is permissible to share and what is not, and the associated controls.

D8. Disclose the full range of purposes for which the organization shares data (including for its core business and additional commercialization purposes).

Reference
SASB Drug Retailers Sustainability Accounting Standard (at HC-DR-230a.1, 2);
EOS;
RDR (at P5)

Commentary
Mobile health companies have opportunities to expand into virtually boundless multi-party networks that share data. The networks may involve connections with the brand's business affiliates and partners, such as advertising vendors, analytics service providers, storage providers, social media platforms, and app developers. Affiliations like these among retailers, technology companies, and other firms in the mobile health market are partly due to the rise of the "partnership economy,"[35] where enterprise-level relationships provide a strategic third channel of business growth next to sales and marketing. Data sharing in health contexts must be evaluated for legal, regulatory, and reputational risk. The potential for downside risk is illustrated by the case of GoodRx, which settled a complaint with U.S. authorities in 2023 in response to allegations that the company shared consumer health data with third parties, despite repeated assurances that it would protect users' privacy.[36] The resulting consent order requires GoodRx to pay a civil penalty of $1.5 million and bans the company from further disclosing health information for advertising purposes or without affirmative consent and notice, among other stipulations.

Data retention

D9. Disclose the duration of time for which the organization retains user information.

Definition
User. See the definition at D2.

Reference
SASB Drug Retailers Sustainability Accounting Standard (at HC-DR-230a.1, 2);
RDR (at P6)

34 Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky, "Mobile Health and Privacy: Cross Sectional Study," *BMJ* 373, no. 1248 (2021): 1–12.

35 David A. Yovanno, *The Partnership Economy* (Hoboken, NJ: Wiley, 2022).

36 U.S. Department of Justice, Office of Public Affairs, "Digital Healthcare Platform Ordered to Pay Civil Penalties and Take Corrective Action for Unauthorized Disclosure of Personal Health Information," (February 22, 2023), https://www.justice.gov/opa/pr/digital-healthcare-platform-ordered-pay-civil-penalties-and-take-corrective-action.

Commentary

By keeping large volumes of old data, companies subject themselves to operational and regulatory risks,[37] as well as human rights risks.[38] Practicing "data minimization" — collecting only the data that is needed, using acquired data only for authorized uses, and retaining as little of that data as possible — has become part of evolving concepts of corporate digital responsibility[39] and is written into some hard law, such as GDPR in the E.U.[40] In the United States, the Federal Trade Commission has begun to impose limits on data retention through Section 5 of the FTC Act and through the Gramm-Leach-Bliley Safeguards Rule.[41] In 2022, the FTC reached a $1.5 million settlement with WW International Inc. (the parent company of Weight Watchers) and a subsidiary based on the complaint that the companies retained children's data for too much time, in addition to other offenses.[42] The companies had been retaining the data for at least three years, even if the user account was dormant. The FTC saw this practice as unacceptable because, under Section 5 of the FTC Act, engaging in unreasonable data security practices, including retaining data for longer than necessary for a legitimate business or legal purpose, is considered an unfair practice.

D10. Disclose the full range of purposes for which the organization retains data (including core business and additional commercialization purposes).

Reference

EOS

Commentary

Knowing the purposes of data retention helps stakeholders weigh the potential financial opportunities against risks. (For more on data retention risks, see the commentary at D9.) Both data value and risk may be proportional to the age of the data, according to Rohan Light, a New Zealand-based consultant and expert in data governance and risk. The older the data assets, the more likely they are overvalued and/or invalid, because both their referents change over time and better methods for analysis are found. This is particularly the case for datasets that are supposed to represent a population but were built on the basis of outmoded procedures that introduce undesirable biases such as racial or gender biases.

37 Avi Gesser, Johanna Skrzypczyk, and Michael R. Roberts, "Data Minimization – Recent Enforcement Actions Show Why Some Companies Need to Get Rid of Old Electronic Records," Program on Corporate Compliance and Enforcement, New York University School of Law (May 26, 2022), https://wp.nyu.edu/compliance_enforcement/2022/05/26/data-minimization-recent-enforcement-actions-show-why-some-companies-need-to-get-rid-of-old-electronic.

38 Eric Null, Isedua Oribhabor, and Willmary Escoto, "Data Minimization: Key to Protecting Privacy and Reducing Harm," Access Now (May 2021), https://www.accessnow.org/press-release/data-minimization-guide/.

39 Christina J. Herden et al., "Corporate Digital Responsibility: New Corporate Responsibilities in the Digital Age," *NachhaltigkeitsManagementForum* 29 (2021): 23.

40 The data minimization principle is expressed in Article 5(1)(c) of the GDPR, which provides that personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed." European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, https://eur-lex.europa.eu/eli/reg/2016/679/oj. The same expression of the data minimization principle is found in Article 4(1)(c) of the data processing regulation for E.U. institutions, agencies, and bodies (Regulation 2018/1725).

41 James Dempsey, "Why FTC's GLB Safeguards Rule Update is Noteworthy," International Association of Privacy Professionals (November 3, 2021), https://iapp.org/news/a/why-ftcs-glb-safeguards-rule-update-is-noteworthy/.

42 Federal Trade Commission, "FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data," (March 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive.

Third-party requests to share user information

D11. Disclose the process for responding to third-party requests (by both government and private parties) to share user information.

Definition

User. See the definition at D2.

Reference

RDR (at P10)

Commentary

Third-party requests to share user information have become part of transparency reporting, a form of corporate disclosure inaugurated by the information and communication technology (ICT) industry in the 2010s.[43] Following revelations of mass surveillance by the U.S. government in 2013, transparency reporting has become an expected channel of public communication among large ICT companies and an indicator of how firms will defend user interests. We anticipate that similar expectations will spread outward to more sectors and markets, including mobile health, with firms expected to provide a description of their process for handling data requests as a baseline. Template users may wish to refer to the principles of the Global Network Initiative (GNI), a multistakeholder platform consisting of ICT companies, civil society organizations, investors, and academics.[44] According to results of our interviews and surveys, companies in the mobile health market should consider disclosing:

- internal procedures for performing diligence on requests;
- procedures for complying with or refusing requests;
- a percentage rate of compliance with past requests;
- a grievance mechanism for observers and/or users whose data has been shared;
- an accountability structure, e.g., management and board oversight;
- the role or named person in charge of the process;
- the number of users whose information was requested by law enforcement; and
- the number of law enforcement requests for user information.

Targeted advertising

D12. Disclose whether the organization conducts robust, systematic risk assessment for targeted advertising policies and practices.

Reference

RDR (at G4)

Commentary

Targeted advertising — a form of online marketing through which ads are shown to consumers based on personal traits, preferences, or past behaviors — is a high-profile issue in public policy, business ethics, and advocacy that will likely remain prominent for some time, given the high volume of activities in the digital economy that support it. Also called behavioral advertising, this form of marketing can lead to pri-

43 Peter Micek and Deniz Duru Aydin, "Non-Financial Disclosures in the Tech Sector: Furthering the Trend," in *The Responsibilities of Online Service Providers*, eds. M. Taddeo and L. Floridi (Springer, 2017), 241–61.

44 Global Network Initiative, "The GNI Principles," accessed June 9, 2023, https://globalnetworkinitiative.org/gni-principles/.

vacy and data protection violations, particularly when companies use unsupervised third-party code like ad trackers.[45] Mobile health companies that work with the advertising technology (adtech) industry — to serve patient-facing drug ads, for example — might intentionally or unintentionally violate anti-discrimination laws. Discriminatory impacts can result from targeting people based on protected characteristics such as disability or race, or by using proxies for protected characteristics, such as purchase history, browsing history, income, or location.[46] This disclosure prompt reflects growing public awareness of the ways that targeted advertising incentivizes interactions among marketers, data brokers, companies in the mobile health market, and their business partners. For example, marketers sell personally identifiable data on mental health conditions — a practice that has been accelerating amid growth in telehealth, therapy apps, and wellness apps.[47]

Companies that perform comprehensive risk assessment for targeted advertising signal to stakeholders that they systematically identify and prioritize hazards that could negatively impact the organization's ability to conduct business. Failure to implement effective policies and processes may expose companies and their shareholders to material legal, regulatory, and reputational risks. A risk assessment should involve, at a minimum, risk identification, prioritization, and action planning. An effective risk assessment should result in action, including creation of risk responses and the set-up of control and monitoring activities.

CYBERSECURITY, C1–C9

Personnel/resources

C1. Disclose whether the organization has a cyber and/or information security team.

Reference

PRI;
WBA (at U1)

Commentary

Companies that share clear communication about their cybersecurity resources provide valuable contextual information that reassures investors, consumers, and others that cybersecurity issues are being managed. In PRI's 2018 survey of 100 companies across IT, telecommunications, healthcare, consumer goods, and financial industries, a quarter of responding companies disclosed that they have a cyber or information security team.[48] Further, the World Benchmarking Alliance evaluates companies on whether they assign accountability for cybersecurity at a senior level, serving to "indicate the appropriate provision of accountability, managerial capacity, and company resources dedicated to prevention, mitigation, and resolution of cybersecurity risks."[49]

45 Scott Ikeda, "Study Finds Medical Apps Are Sharing Health Data With Third Party Trackers, Funneling Info to Targeted Facebook Ads," *CPO Magazine* (August 25, 2022), https://www.cpomagazine.com/data-privacy/study-finds-medical-apps-are-sharing-health-data-with-third-party-trackers-funneling-info-to-targeted-facebook-ads/.

46 Bennett Cyphers and Adam Schwartz, "Ban Online Behavioral Advertising," Electronic Frontier Foundation (March 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising.

47 Drew Harwell, "Now for Sale: Data on Your Mental Health," *Washington Post* (February 13, 2023), https://www.washingtonpost.com/technology/2023/02/13/mental-health-data-brokers/.

48 U.N. Principles for Responsible Investment, "Stepping Up Governance on Cyber Security: What is Corporate Disclosure Telling Investors?" (2018), 10, https://www.unpri.org/governance-issues/stepping-up-governance-on-cyber-security/3452.article.

49 World Benchmarking Alliance, "Digital Inclusion Benchmark Methodology Report," (April 2020), 29, available at https://www.worldbenchmarkingalliance.org/publication/digital-inclusion/methodology/.

Incidents & response

C2. Disclose whether the organization has established an incident management plan that includes plans for disaster recovery and business continuity.

Reference
PRI

Commentary
Cyberattacks pose a significant business risk, and a company's capacity to recover and return to normal operations is crucial to enterprise survival. Companies should disclose whether they have an incident management plan intended to minimize and contain damage, and to facilitate rapid recovery. In PRI's 2018 survey of 100 companies across IT, telecommunications, healthcare, consumer goods, and financial industries, half responded that they disclose their disaster recovery and business continuity plans to investors and other stakeholders. We expect the frequency of this practice to rise. Regulators in many jurisdictions require companies to disclose data breaches within short timeframes — three or four days in some cases — putting extreme pressure on timely compliance for those companies that lack an incident management plan, explained Shannon Yavorsky, partner at Orrick Herrington & Sutcliffe LLP.

C3. Disclose material cybersecurity incidents.

Definitions
Material. Because "material" is an operative term in securities law and regulation with different meanings across jurisdictions, and because "material" has taken on new meanings with the rise of ESG and other nonfinancial reporting, companies should specify which definition they are using when disclosing through this template.

Cybersecurity incident. Because many jurisdictions around the world have breach notification laws, companies should specify which definition they are using when disclosing incidents through this template.

Reference
EOS;
WBA (at U2)

Commentary
Cybersecurity incidents can upset business operations, create legal and regulatory risks, and set into motion adverse human rights and equity impacts, such as privacy infringements and loss of opportunity. While incidents are firmly seen as a governance issue in ESG, they are also beginning to be appreciated as a social issue. How much privilege individuals have significantly affects their ability to weather the consequences of a data breach.[50] Low-income populations are less resilient to resulting financial harms that emerge after a breach leads to identity theft.[51] With regard to reporting, a number of jurisdictions and exchanges already have breach notification laws or continuous disclosure requirements. For example, companies listed on the Australian Securities Exchange must disclose information about a cybersecurity incident if "a reasonable person would expect [it] to have a material effect on the price or value of the

50 Alice E. Marwick and danah boyd, "Understanding Privacy at the Margins," *International Journal of Communication* 12 (2018): 1157–65.

51 Ryan Whirty, "Questions Loom Over Impact of Data Breach on Vulnerable Communities," *The Louisiana Weekly* (Aug. 26, 2019): 9.

entity's securities."[52] Further, companies that are periodic filers with the U.S. Securities and Exchange Commission (SEC) are preparing for new disclosures to be mandatory. The SEC's new requirements for cyber reporting, adopted in July 2023, generally require registrants to disclose material cybersecurity incidents within four business days on Form 8-K, and foreign private issuers must make comparable disclosures on Form 6-K.[53] Our template encourages companies to reduce information asymmetry regarding material incidents through appropriate disclosure.

C4. Disclose the number of users affected by data breaches.

Definitions

User. See the definition at C2.

Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or is reasonably believed to have accessed information; or an authorized user accesses information for unauthorized purpose. [Adapted from the National Institute of Standards and Technology's Computer Security Resource Center Glossary.[54]]

- We substituted "information" for "personally identifiable information" when adapting the NIST definition, since companies and investors are interested in breaches of other important data, such as intellectual property.
- We substituted "is reasonably believed to have accessed" for "potentially accesses" when adapting the NIST definition, since this change makes it absolutely clear that there need not be definitive confirmation of unauthorized activity. (For the "reasonably believed" language, compare California's breach notification statute.[55])

Reference

SASB Internet Media & Services Sustainability Accounting Standard (at TC-IM-230a.1)

Commentary

Of particular relevance to investors, the aggregate number of users impacted by data breaches contributes to assessment of downstream financial risks and potential adverse impacts to equity and human rights. For example, Australian private insurer Medibank — which participates in the mobile health market through its My Medibank and Live Better apps[56] — faces a class action lawsuit after a 2022 cyber attack resulted in personal details of up to 10 million customers being posted on the dark web.[57] Reporting

52 Australian Securities Exchange, "ASX Listing Rules," Chapter 3: Continuous Disclosure, available at https://www2.asx.com.au/about/regulation/rules-guidance-notes-and-waivers/asx-listing-rules-guidance-notes-and-waivers, accessed June 16, 2023.

53 U.S. Securities and Exchange Commission, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," (July 26, 2023), https://www.sec.gov/news/press-release/2023-139.

54 National Institute of Standards and Technology, Computer Security Resource Center Glossary, "Breach," accessed June 16, 2023, https://csrc.nist.gov/glossary/term/breach.

55 California Legislative Information, California Civ. Code § 1798.82(a), https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

56 Medibank, "Live Better, Get Rewarded," accessed June 16, 2023, https://www.medibank.com.au/livebetter/rewards/.

57 Josh Taylor, "Medibank Class Action Launched After Massive Hack Put Private Information of Millions on Dark Web," *The Guardian* (February 15, 2023), https://www.theguardian.com/australia-news/2023/feb/16/medibank-class-action-launched-data-breach-private-information-dark-web.

organizations might wish to append a description of corrective actions implemented in response to breaches, in order to align with SASB standards prescribing disclosure of that information.[58]

C5. Disclose the percentage of data breaches involving personal information.

Definitions

Breach. See the definition at C4.

Personal information. Adapted from the California Consumer Privacy Act (as amended by the California Privacy Rights Act),[59] "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under law applicable to the company and its operations;
- Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website or application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information, defined as personally identifiable information that is not publicly available;
- Inferences drawn from any of the information identified in this definition to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes;
- Sensitive personal information, which is:
    - Personal information that reveals:
        - A consumer's social security, driver's license, state identification card, or passport number;
        - A consumer's account log-in, financial account, debit card, or credit card number, in combination with any required security or access code, password, or credentials allowing access to an account;
        - A consumer's precise geolocation;

58 For example, see Sustainability Accounting Standards Board, Internet Media & Services Sustainability Accounting Standard, TC-IM-230a.1, p. 6 n. 4.

59 California Legislative Information, "California Consumer Privacy Act of 2018, CA Civil Code § 1798.100," (2018), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

- A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, email, and text messages, unless the business is the intended recipient of the communication; and
- A consumer's genetic data;

—or—

- The processing of biometric information for the purpose of uniquely identifying a consumer;

—or—

- Personal information collected and analyzed concerning a consumer's health;

—or—

- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

Of note, sensitive personal information that is "publicly available" is excluded from this definition.

Reference
SASB Health Care Delivery Sustainability Accounting Standard (at HC-DY-230a.3)

Commentary
Breaches of personal information, as opposed to other kinds of information held in company systems, have distinct consequences. They are tightly linked to legal and regulatory risk, and to impacts to equity and human rights. Personal information plays a prominent role in comprehensive privacy and data protection laws such as the Brazilian General Data Protection Law, but also civil rights and human rights laws, and social norms regarding non-discrimination and individual autonomy. Reporting organizations should append a description of corrective actions implemented in response to breaches in order to align with SASB standards prescribing disclosure of that information.[60]

C6. Disclose the percentage of data breaches involving consumer health data.

Definition
Breach. See the definition at C4.

Consumer health data. Adapted from Washington state's My Health My Data law,[61] consumer health data is personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status.

- For purposes of this definition, physical or mental health status includes, but is not limited to:
  - Individual health conditions, treatment, diseases, or diagnosis;
  - Social, psychological, behavioral, and medical interventions;
  - Health-related surgeries or procedures;
  - Use or purchase of prescribed medication;
  - Bodily functions, vital signs, symptoms, or measurements of the information described in this definition;

60 For example, see Sustainability Accounting Standards Board, Internet Media & Services Sustainability Accounting Standard, TC-IM-230a.1, p. 6 n. 4.

61 Washington State Legislature, "HB 1155 – 2023-24," available at https://app.leg.wa.gov/billsummary?BillNumber=1155&Year=2023.

  - Diagnoses or diagnostic testing, treatment, or medication;
  - Gender-affirming care information;
  - Reproductive or sexual health information;
  - Biometric data;
  - Genetic data;
  - Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
  - Data that identifies a consumer seeking health care services;
  - Any information that a business or their processor processes to associate or identify a consumer with the data described above that is derived or extrapolated from non-health-related information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

- "Consumer health data" does not include personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or similar independent oversight entity that determines that the organization has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

Reference

SASB Health Care Delivery Sustainability Accounting Standard (at HC-DY-230a.3)

Commentary

There is growing recognition that "consumer health data" encompasses kinds of information that ought to be protected, even if it is collected or used outside traditional healthcare delivery, pharmacy, and insurance contexts.[62] Further, it is becoming more widely appreciated that the inference economy and machine learning make it possible to generate sensitive health-related information from aggregations of seemingly innocuous data.[63] As we see policymakers shift in response to these developments, companies should prepare to report on the percentage of data breaches involving consumer health data. Reporting organizations might wish to append a description of corrective actions implemented in response to breaches in order to align with SASB standards prescribing disclosure of that information.[64]

C7. Disclose the number of breaches of customer data.

Definition

Breach. See the definition at C4.

Reference

GRI (at 418-2)

62 Thomas German, "Mental Health Apps Aren't All As Private As You May Think," *Consumer Reports* (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/; Vivian Genaro Motti and Shlomo Berkovsky, "Healthcare Privacy," in *Modern Socio-Technical Perspectives on Privacy*, ed. B. P. Knijnenburg, X. Page, P. Wisniewski, H. R. Lipford, N. Proferes, J. Romano (Cham: Springer, 2022), 203–31.

63 Alicia Solow-Niederman, "Information Privacy and the Inference Economy," *Northwestern University Law Review* 117 (2022): 357–424.

64 For example, see Sustainability Accounting Standards Board, Internet Media & Services Sustainability Accounting Standard, TC-IM-230a.1, p. 6 n. 4.

Commentary
Breaches of customer data were identified by our expert panel as critical for disclosure. Although breaches of employee, intellectual property, and other categories of business data can have significant consequences, customer data is singled out for special reporting. When disclosing through this template, companies may distinguish between B2B (business-to-business) and B2C (business-to-consumer) customers.

Resilience

C8. Disclose how the organization addresses security vulnerabilities when they are discovered.

Reference
RDR (at P14)

Commentary
This disclosure offers companies and investors some discretion about how they communicate priorities to address known security vulnerabilities. PRI's 2018 study provides some sample disclosures from firms in different industries, such as descriptions of their:

- collaboration with the national cybersecurity emergency response team in the jurisdiction where they are headquartered;
- communication with industry information-sharing centers;
- access to external expertise through third-party vendors, consultants, or customers; or
- action plans for better implementation of the firm's cybersecurity strategy.[65]

This disclosure can help companies fulfill the GRI 3-3 reporting standard, which calls for description of actions taken to manage each material topic and related impacts, as companies in technology-focused verticals such as mobile health continue to identify cybersecurity as a material issue. For example, the GRI index in Medtronic's 2022 Integrated Performance Report states that, to manage technology and device security, the company publicly discloses security vulnerabilities through its Coordinated Disclosure Process and includes a link to a landing page for this process, which invites communications from the security research community about potential vulnerabilities in Medtronic products and services.[66] The company's report adds that, in FY22, Medtronic "disclosed six security vulnerabilities, which included security bulletins, updates to previous bulletins, and security notices responding to third-party risks that may not be applicable to Medtronic but helped address customer inquiries."[67]

C9. Disclose a description of policies and practices used to secure customers' consumer health data and other personal information.

Definitions
Consumer health data. See the definition at C6.

Personal information. See the definition at C5.

65 U.N. Principles for Responsible Investment, "Stepping Up Governance on Cyber Security: What is Corporate Disclosure Telling Investors?" (2018), 11–12, https://www.unpri.org/governance-issues/stepping-up-governance-on-cyber-security/3452.article.
66 Medtronic, 2022 Integrated Performance Report, 116, referring to https://global.medtronic.com/xg-en/product-security/coordinated-disclosure-process.html.
67 Ibid.

Reference
SASB Drug Retailers Sustainability Accounting Standard (at HC-DR-230a.1)

Commentary
Companies should report the nature, scope, and implementation of their policies and practices related to securing consumer health data and personal information. Following guidance provided in SASB Standards, companies should organize their description by stages in the information lifecycle, including collection, use, retention, processing, disclosure, and destruction.[68] Companies should be prepared to track broadly defined categories of consumer health data and personal information, in line with widening regulatory definitions. For example, some investors want to know about policies and practices that go beyond HIPAA protections under U.S. law, since only a very limited number of entities and data practices are in scope. "There are a lot of privacy concerns with personal health information that go beyond HIPAA," explained Lydia Kuykendal, director of shareholder advocacy at Mercy Investment Services. "Don't come at me with 'We protect HIPAA information.' That's a really specific set of data, and under really specific circumstances."

ARTIFICIAL INTELLIGENCE, A1–A5

Policy

A1. Disclose the organization's policy for AI governance.

Definition
AI (*see also algorithmic system below*). The definition of AI (artificial intelligence) will need flexibility to change over time because of technological and cultural developments. This template does not offer one single definition of AI but follows the United Nations Educational, Scientific, and Cultural Organization (UNESCO) by offering an approach to understanding AI systems as "information-processing technologies that integrate models and algorithms that produce a capacity to learn and to perform cognitive tasks leading to outcomes such as prediction and decision-making in material and virtual environments. AI systems are designed to operate with varying degrees of autonomy by means of knowledge modeling and representation and by exploiting data and calculating correlations. AI systems may include several methods, such as but not limited to:

(i) machine learning, including deep learning and reinforcement learning;
(ii) machine reasoning, including planning, scheduling, knowledge representation and reasoning, search, and optimization."[69]

Reference
EOS;
Equal AI Checklist;
RDR (at F12)

Commentary
Publishing an AI policy is a key action that companies can take "that signals to people that the company has taken AI seriously and its use within the organization seriously such that they've promulgated a responsive policy," said Shannon Yavorsky, partner at Orrick Herrington & Sutcliffe LLP. Propelling the need for

68 See Sustainability Accounting Standards Board, Drug Retailers Sustainability Accounting Standard (2018), HC-DR-230a.1.2.
69 UNESCO, "Recommendation on the Ethics of Artificial Intelligence," (Paris: UNESCO, 2022), https://unesdoc.unesco.org/ark:/48223/pf0000381137.

policy is generative AI, the headline-grabbing technologies that use algorithms to create new content from existing materials, such as text, audio, images, video, and code. A growing number of companies will need to establish protocols for the design, deployment, procurement, monitoring, and employee use of AI as appropriate, and determine which AI systems their policy applies to. Furthermore, companies need to assess whether policies are tagged with "responsible AI," "ethical AI," "AI ethics," or similar headings to indicate normative approaches, and whether the policy document will take the form of a commitment, a set of principles, or something else. Investors and civil society organizations are increasingly urging companies to disclose their policies for using AI. A collaborative initiative organized by World Benchmarking Alliance produced an "Investor Statement on Ethical AI" in 2022 calling on companies to disclose "a commitment to abide by principles for ethical AI development and application," and launched an investor engagement representing more than $6.3 trillion in assets under management or advice.[70]

Practices

A2. Disclose the range of purposes for which algorithmic systems are used.

Definition

Algorithmic system (*see also AI above*). An algorithmic system is a set of algorithms. According to the Association for Computing Machinery (2017), an algorithm is "a self-contained step-by-step set of operations that computers and other 'smart' devices carry out to perform calculation, data processing, and automated reasoning tasks. Increasingly, algorithms implement institutional decisionmaking based on analytics, which involves the discovery, interpretation, and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance."[71]

Reference

EOS

Commentary

This disclosure helps companies, investors, oversight bodies, and other stakeholders assess which legal and regulatory requirements apply to use of algorithmic systems, since context of use — and risk level associated with that context — are central factors in how applicable law is scoped. For example, Canada's proposed Artificial Intelligence and Data Act would require businesses that design, develop, deploy, or manage high-impact AI systems to create a mitigation plan to reduce risks and increase public reporting.[72] Further, the E.U.'s proposed regulatory framework for AI would establish obligations for providers and users depending on the level of risk to health, safety, or fundamental rights — with risk levels designated as "minimal," "limited," "high," or "unacceptable."[73] One or both of these developing regulations could impose heightened requirements for companies in the mobile health market through

70 World Benchmarking Alliance, "Investor Statement on Ethical AI," (April 26, 2022), https://www.worldbenchmarkingalliance.org/impact/investor-statement-on-ethical-ai/.

71 Association for Computing Machinery US Public Policy Council and Europe Council, "Statement on Algorithmic Transparency and Accountability," (updated May 25, 2017), https://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf.

72 Innovation, Science and Economic Development Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion Document," (last modified March 13, 2023), https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s1.

73 European Commission, "Regulatory Framework Proposal on Artificial Intelligence," (last modified June 20, 2023), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

such AI-powered applications as chatbots; predictive systems based on biometric, physical, or behavioral data of individuals; content recommendation systems; or systems critical to health and safety.

Moreover, a disclosed range of purposes will help stakeholders distinguish between scientific and pseudoscientific claims of companies in order to assess legal, regulatory, and reputational hazards. This mode of distinction is of special importance in segments of the mobile health market, such as companies that offer diagnostic, predictive, or therapeutic systems. For example, stakeholders should be able to evaluate whether a given algorithmic system fits into ethics controversies about technologies that make predictions about people based on their physical or behavioral characteristics.[74]

A3. Disclose how the organization takes action to eliminate racial, gender, and other biases in algorithms.

Definition

Algorithm. See the definition of *algorithmic system* at A2.

Reference

EOS;
EqualAI

Commentary

One of the controversies that propelled AI bias into public awareness was a healthcare algorithm: a commercial algorithm used by health services innovation company Optum assigned Black patients the same level of risk as White patients, even though the former had more chronic health conditions.[75] Authors of the breakthrough study of this algorithm estimated that racial bias, built into the algorithm through the data it consumed as it was trained, reduced the number of Black patients identified for extra care by more than half.[76] In a related development, discriminatory bias in AI systems has stoked investor concern in the form of shareholder campaigns and resolutions, some of which have called on prominent technology companies to perform racial equity audits or civil rights audits.[77] "We need to know what the guardrails are and whether or not they're being effective because these companies are investing . . . in AI, and then they're also investing in racial justice. Are these dollars being well spent, or are they canceling each other out?" explained Lydia Kuykendal, director of shareholder advocacy at Mercy Investment Services. Mobile health companies should be able to demonstrate practices, policy effectiveness, and/or outcomes regarding mitigation of AI bias against systemically marginalized groups. Interviewee Jian Gong of Better Therapeutics observed that bias in AI models for health applications "could have life or death implications in terms of how you treat certain patients of one race, one gender, and so on."

74 Luke Stark and Jevan Hutson, "Physiognomic Artificial Intelligence," *Fordham Intellectual Property, Media & Entertainment Law Journal* 32, no. 4 (2022): 922–78, https://ir.lawnet.fordham.edu/iplj/vol32/iss4/2.

75 Quinn Gawronski, "Racial Bias Found in Widely Used Health Care Algorithm," *NBC News* (updated November 7, 2019), https://www.nbcnews.com/news/nbcblk/racial-bias-found-widely-used-health-care-algorithm-n1076436.

76 Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan, "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366, no. 6464 (2019): 447–53, https://doi.org/10.1126/science.aax2342.

77 Levi Sumagaysay, "Two Years After George Floyd's Killing, Big Tech Shareholders Vote on Racial-Justice Proposals," *MarketWatch* (updated May 25, 2022), https://www.marketwatch.com/story/two-years-after-george-floyds-killing-big-tech-shareholders-continue-racial-justice-push-11653324711.

A4. Disclose whether the organization conducts human rights due diligence to identify and mitigate the potential risks of algorithmic systems.

Definitions

Human rights due diligence. The essential elements of human rights due diligence are described in the United Nations Guiding Principles on Business and Human Rights (UN GPs) at Principles 17–21.[78] We add that, despite the authoritative guidance, tradeoffs are inherent to the process. Diana Glassman, Director–Engagement at EOS at Federated Hermes, provided an investor perspective on human rights and technology: "There are lots of questions about, whose human rights? And how do you make these tradeoffs? . . . For example, the human rights community that is visible at least to investors has not, in fact, prioritized children." Compromises and prioritization should be disclosed where appropriate.

Algorithmic system. See the definition at A2.

Reference

RDR (at G4)

Commentary

Companies are expected to conduct human rights due diligence across business activities and relationships under the United Nations Guiding Principles on Business and Human Rights (UN GPs), the leading global standard for addressing human rights harms related to business.[79] In the E.U., the proposed Corporate Sustainability Due Diligence Directive (CS3D) would establish a duty for large E.U. companies and some foreign companies to identify, mitigate, and account for negative human rights impacts in their operations, subsidiaries, and value chains.[80] Algorithm-supported decision-making has been linked to elevated human rights risks by organizations such as the United Nations Human Rights B-Tech Project. We suggest that companies and investors working with the present disclosure prompt be guided by the B-Tech Project's engagement tool, "Human Rights Risks in Tech: Engaging and Assessing Human Rights Risks Arising from Technology Company Business Models" (2023), which features a section on algorithmic systems.[81] Further, B-Tech published a 2022 commentary[82] on human rights due diligence, with illustrations from technology companies and special focus on impacts not only in a company's own operations and supply chains, but also downstream, which can be instructive for companies and investors active in the mobile health market.

A5. Disclose whether the organization conducts robust, systematic risk assessment for algorithmic systems.

Definition

Algorithmic system. See the definition at A2.

78 United Nations Office of the High Commissioner for Human Rights, "Guiding Principles on Business and Human Rights," (2011), available at https://digitallibrary.un.org/record/720245.

79 Ibid.

80 European Commission, "Corporate Sustainability Due Diligence," (updated February 23, 2022), https://commission.europa.eu/business-economy-euro/doing-business-eu/corporate-sustainability-due-diligence_en.

81 See Card 2, pp. 10–11 in United Nations Human Rights B-Tech Project, "Human Rights Risks in Tech: Engaging and Assessing Human Rights Risks Arising from Technology Company Business Models" (2023), https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/20230329-B-Tech_Investor_Engagement_Tool.pdf.

82 United Nations Human Rights B-Tech Project, "The Feasibility of Mandating Downstream Human Rights Due Diligence: Reflections from Technology Company Practices," (September 2022), https://www.ohchr.org/sites/default/files/documents/issues/business/2022-09-13/tech-downstream-hrdd.pdf.

Reference
WEF;
RDR (at G4)

Commentary
Companies that perform comprehensive risk assessment for algorithmic systems signal to stakeholders that they systematically identify and prioritize hazards that could negatively impact the organization's ability to conduct business. Risk needs to be handled at the operational, managerial, and strategic levels. Responsibility for risk management starts with the board or a board-level committee. Companies and investors should communicate about the board's capacity to oversee assessment of AI-related risk. There is a perception among investors that there is generally insufficient board-level expertise on AI, explained Navishka Pandit, engagement associate at EOS at Federated Hermes. "I think that speaks to how late we are in being able to get relevant board-level expertise compared to how quickly the company is actually making those [AI-related] changes or investing in that space or entering in that space," Pandit said. In a 2022 survey of 500 executives at American large-cap companies across industries, just 41 percent of respondents reported that their organizations have expertise on AI at the board level.[83]

83 Baker McKenzie, "Risky Business: Identifying Blind Spots in Corporate Oversight of Artificial Intelligence," (March 30, 2022), available at https://www.bakermckenzie.com/en/newsroom/2022/03/bm-survey-artificial-intelligence.

Looking Ahead

LIMITATIONS

Although this work is a major first step toward defining a set of critical disclosures for cutting-edge technology topics, the approach has some limitations that open up opportunities for future research.

Future studies could validate the master list of 26 disclosures and the auxiliary material found in the Definitions and Commentary subsections of this report. A central goal of this study was to select and systematize the most critical disclosure recommendations from authoritative sources in the private and non-profit sectors, but further research and collaboration are needed to test the results against practical constraints that may be related to organizational behavior, risk appetite, data availability, or external factors such as regulatory change. For example, the level of detail for each disclosure was not specified empirically by participants in this study, leaving this a potential topic for a future effort.

With its intentionally small and targeted sample, this study makes no claim to be representative. Selection effects may be at play; in other words, this research may have attracted participants with strong views about practices or philosophies relevant to the study topic, and furthermore it is limited by its use of purposive sampling, a non-probability technique.

The results of this study should be treated as a living document. We invite updates by the scholarly, business, and advocacy communities in step with developments in market conditions, regulation, technology, and normative pressures on businesses.

CONCLUSIONS

The output of this study is an empirically sourced, practical template that can be a starting point for companies and investors who want to be leaders in implementing standardized disclosure for digital responsibility in the areas of data governance, cybersecurity, and AI. The template is downloadable at https://cltc.berkeley.edu/publication/corporate-reporting-template. Users are free to share, remix, transform, and build upon the template under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. Wide adoption of the disclosures recommended in the template would work toward resolving challenges in the corporate reporting landscape, such as questionnaire fatigue among companies

and information overload among investors, that currently impede stakeholder confidence in corporate digital responsibility.

Looking ahead, this work can support constructive dialogue and the continued development of reporting standards. Expansions of this work to different industries and verticals would support advances in industry-based approaches to the SASB Standards. The IFRS Foundation has committed to building on SASB's industry-based approach, which has produced guidance for 77 industries to date.[84] Further, our study is compatible with the modular reporting system administered by the other leading global standard-setter, Global Reporting Initiative. Under GRI's universal standards, organizations must report on material topics, and we anticipate that a growing number will find that data governance, cybersecurity, and/or AI are interconnected with this requirement. Moreover, our results could inform GRI's future work on sector-specific and topical standards. For example, this study suggests refinements for existing topic standards like Customer Privacy and helps establish foundations for new standards being developed by GRI's Sector Program, which has prioritized 40 sectors.[85]

More broadly, this work can support dialogue among private, public, and non-profit organizations that shape corporate disclosure norms. New developments in technology and stakeholder views not represented in this work will need to be incorporated. Adaptations for different markets, verticals, and industries will need to be made. There may be uses for this template outside our primary objectives, such as informing new legislative proposals, B2B (business-to-business) risk management, benchmarking exercises, or the updating of listing requirements and guidelines by stock exchanges.

84 SASB Standards: Now Part of IFRS Foundation, "Standards Overview," accessed June 14, 2023, https://sasb.org/standards/.
85 Global Reporting Initiative, "Sector Program," accessed June 14, 2023, https://www.globalreporting.org/standards/sector-program/.

Appendix A: Study Methodology

OVERVIEW

The aim of this study was to establish a process to bring a panel of 20 experts to a degree of consensus regarding critical disclosures on data governance, cybersecurity, and AI that companies in the mobile health market should make. To augment the results with commentary and examples, the researcher conducted semi-structured interviews with select participants. Jordan Famularo, PhD, Postdoctoral Scholar at the Center for Long-Term Cybersecurity, was the sole researcher.

The study protocol was submitted for review by the University of California, Berkeley's Office for Protection of Human Subjects. Exemption was granted, effective from April 19, 2023 to April 18, 2033 (CPHS # 2023-03-16202). The approval letter is on file with the author.

RECRUITMENT

The recruitment process occurred in March and April 2023. To capture a broad range of perspectives, the recruitment targeted participants from institutional investors, law firms, consultancies, companies providing mobile health products and/or services, academia, and non-profit organizations. Famularo identified potential subjects using purposive sampling, a non-probability selection based on judgment of their role in an organization, their capacity to assess corporate reporting priorities, and their ability to elucidate study themes. Two methods for the sampling were used. First, Famularo used public profiles, such as online biographies and LinkedIn profiles, some of which were found through desk research on organizations involved in published grey literature or events related to the study topic. Second, peer recruitment using an electronic invitation was used.

Prospective participants received initial contact through email or LinkedIn direct message. They received information about the nature of the study, confidentiality, the names of the sponsoring university and external funder, and the expected time commitment. Prior to participation, subjects gave consent through the initial screen of the first online survey and, if contributing to the interview portion of the study, they gave consent in electronically transmitted

writing. For both the surveys and the interviews, a consent form was created using the Office for Protection of Human Subjects' suggested template.

PARTICIPANTS

The panel of 20 experts assembled for the Delphi study was composed of professionals from eight countries and varied domains in the private and non-profit sectors. Below is a summary of their geographic and occupational range:

Professional domains (total = 20 participants)
6 advisory/consulting firms
3 institutional investors
1 pharmaceutical company
2 technology companies
5 non-profit organizations
1 law firm
2 academia

Locations (total = 20 participants)
1 Australia
1 Belgium
2 Canada
1 Italy
1 Japan
1 New Zealand
2 Switzerland
11 United States

Each individual's participation in the Delphi study was for empirical purposes only and does not imply endorsement of this report or the accompanying template. Observations, conclusions, and recommendations are made solely by the author.

Delphi study participants:
Andrea Bonime-Blanc (GEC Risk Advisory)
Andrew (Andy) Behar (As You Sow)
Audrey Mocle (Open MIC [Open Media and Information Companies Initiative])
Chris McClean (Avanade)
Diana Glassman (EOS at Federated Hermes)
Jian Gong (Better Therapeutics)
Jordan Wrigley (Future of Privacy Forum)
Lisa Thee (Launch Consulting)
Lydia Kuykendal (Mercy Investment Services)
M. Alejandra Parra-Orlandoni*
Matteo Giglioli*
Maya Bundt (Swiss Risk Association)
Meredith Veit (Business and Human Rights Resource Centre)
Navishka Pandit (EOS at Federated Hermes)
Raphael Reischuk (Swiss National Test Institute for Cybersecurity NTC)
Rohan Light*
Shannon Yavorsky (Orrick Herrington & Sutcliffe LLP)
Stephen Pitt-Walker (Optima Board Services; Governance Institute of Australia)
Theresa Miedema (Ontario Tech University)
One anonymous participant

** In professional capacity independent of current affiliation.*

GROUP COMMUNICATION PROCESS

This study used a Delphi technique, a method for achieving convergence of opinion solicited from experts concerning their real-world knowledge.[86] The technique is commonly used for conducting detailed examinations and discussions of a specific issue for the purpose of forecasting, goal-setting, or policy investigation. The objective was to correlate informed judgments spanning a wide range of disciplines about which disclosures should be made. The group communication process has some characteristic features, three of which were key to this research:

1. The researcher deploys multiple iterations of surveys or questionnaires;
2. The researcher provides confidentiality to respondents; and
3. The researcher administers controlled feedback at intermediate points in the study.

The feedback process had two main parts. First, surveys were issued in three iterations, with the second and third building on the round previous to it. Surveys 2 and 3 provided respondents with aggregate group-level results from the prior round so that, if they wished, they could use that information to reassess their answers to reissued questions.

As is typical with Delphi studies, the feedback process and confidential response channel were designed to offset the shortcomings of pooling opinions in real-time group interaction (e.g., influences of dominant personalities, group pressure for conformity, and other biases not related to the study purpose).

Surveys asked participants to respond to 87 distinct disclosure prompts, some of which were issued in more than one survey round, using a common format. This was an identical question and answer set combined with a different disclosure prompt [shown here in brackets]:

Example

How important is it for companies in the consumer-facing mobile health market to disclose [the range of purposes for which algorithmic systems are used]?

- critical
- somewhat important
- somewhat unimportant
- not at all important
- don't know

86 Hsu and Sandford, "The Delphi Technique: Making Sense of Consensus," *Practical Assessment, Research & Evaluation* 12, no. 10 (2007): 1–8.

Respondents were primed at the start of each thematic subsection with the following message:

> The context we'd like you to have in mind is:
> investor demand for material financial information
> and
> investor concerns about human rights and equity that could also impact companies' financial performance.

Several design decisions were intended to mitigate bias and reduce survey fatigue. The sequence of questions was randomized within blocks (or subthemes), which were subordinated under the three main themes of data governance, cybersecurity, and AI. Within each block, question order was fixed because some prompts had very similar but distinct language, which tended to reduce survey fatigue when the questions were presented immediately next to each other.

Famularo collected and analyzed the results of Survey 1 to design Survey 2. She retained each disclosure item if >60 percent of respondents agreed that it is critical.[87] Retained items went onto a master list of critical disclosures. Items that yielded between 40–60 percent agreement on their critical status were considered mixed results and retested in the next round. Items that received <40 percent agreement were discarded. A similar design converted the results of Survey 2 to a design for Survey 3. Disclosure items that yielded >60 percent agreement as critical were retained and placed on the master list. The retest requirement was heightened for this round. Items that yielded 50–60 percent agreement on their critical status were retested in Survey 3. Items that received <50 percent agreement were discarded. At the end of Survey 3, Famularo again retained any disclosure items that had >60 percent agreement on their critical status; she added these to the master list. The remaining items were observed to yield mixed results or low results using the same thresholds as the previous round.

In sum, the survey series generated a final set of 26 critical disclosures, which form the basis for the reporting template. This number reflects one consolidation of two disclosures into one (D1), which is described in the report at p. 16, reflecting a drop in the total to 26 from 27. Sequential results are summarized below:

87 In the academic literature making use of Delphi studies, thresholds for consensus differ, ranging from as low as 51% agreement among respondents to 80%. See Felicity Hasson, Sinead Keeney, and Hugh McKenna, "Research Guidelines for the Delphi Survey Technique," *Methodological Issues in Nursing Research* 32, no. 4 (2000): 1011.

Survey 1 Results: High-Level Summary

19 participants responded to 83 distinct disclosures
Response rate: 95 percent
15 disclosures rose to the top as critical (>60 percent)
28 disclosures fell off as less than critical (<40 percent)
40 disclosures gave mixed results about whether they are critical to disclose (40-60 percent)

Survey 2 Results: High-Level Summary

15 participants responded to 44 distinct disclosures
Response rate: 75 percent
7 disclosures rose to the top as critical (>60 percent)
22 disclosures fell off as less than critical (<50 percent)
15 disclosures gave mixed results about whether they are critical to disclose (50-60 percent)

Survey 3 Results: High-Level Summary

17 participants responded to 15 distinct disclosures
Response rate: 85 percent
6 disclosures rose to the top as critical (>60 percent)
3 disclosures fell off as less than critical (<50 percent)
6 disclosures gave mixed results about whether they are critical to disclose (50-60 percent)

Surveys were conducted via Qualtrics, a web-based application, using the university's license. Three rounds of surveys were conducted from April to May 2023. For each round, respondents had 10 days to submit their surveys. Survey data was stored on the Qualtrics platform.

INTERVIEWS

Interviews took place on Zoom between April and May 2023. They were semi-structured, carried out by Famularo using an interview guide. Nine selected participants agreed to eight interviews (one of which was joint with two interviewees). The primary domains of the interviewees were: one non-profit, three consultancies, one technology company, three institutional investors, and one law firm. The duration of each interview was approximately 45 minutes. The audio was recorded and transcribed with software. Transcripts were then stored with the university's

licensed web application for storage, Box, which is password-protected. With the transcripts securely stored, the recordings were deleted.

To analyze the interview content, Famularo coded the notes using qualitative coding software Atlas.ti. After finalizing the coding, Famularo visualized aggregate results in Atlas.ti. These aggregate results and individual segments of interview notes were the basis for the interpretation in this guide.

RESULTS

The survey series generated a final set of 26 critical disclosures, which form the basis for the reporting template, which is contextualized with observations from the eight interviews. The 26 disclosure items consist of 12 data governance (D) disclosures, nine cybersecurity (C) disclosures, and five AI (A) disclosures. For ease of reference, we grouped them by theme and assigned each an identifier (D1–D12, C1–C9, and A1–A5).

Updates to Definitions

Some terminology clarifications and revisions were necessary to build an effective template, for two key reasons. First, most disclosure items (73/87) were adapted from language found in sources published before 2021, with one exception published in 2022. Due to technological, policy, and cultural shifts, some key terms from the sources needed to be replaced or their definitions updated. Second, the effort to harmonize recommendations from multiple sources presented some inconsistencies in terminology.

Below are the primary terminology clarifications inserted after the data collection phase, based on the researcher's review of all survey and interview content.

Breach. See the updated definition below at C4 (p. 25). To streamline aspects of cybersecurity reporting, the template gives a single definition of "breach." This decision partly arises from the fact that definitions of breach, loss, theft, and leak — referring to cybersecurity incidents — are not harmonized in previous voluntary reporting guidelines such as SASB and GRI standards. We consolidate similar terms into the umbrella concept "breach."

Personal information and consumer health data. See updated definitions below at C5 and C6 (pp. 26–27). In the standard-setting literature, the terms "personally identifiable information"

and "protected health information" appear in some of the metrics published by SASB in 2018. Our study participants identified three of these metrics as critical for companies and investors in the mobile health market:

1. Disclose the percent of data breaches involving personally identifiable information (PII).[88]
2. Disclose the percent of data breaches involving protected health information (PHI).[89]
3. Disclose a description of policies and practices to secure customers' protected health information (PHI) records and other personally identifiable information (PII).[90]

To update these disclosure prompts for 2023, we first recognize that SASB's cited definitions for PII and PHI are now out of step with current parlance. Its definition of PII relies on a 2008 source, the *U.S. Government Accountability Office's Report to Congressional Requesters, Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, and its definition of PHI draws on a 1996 law, the U.S. Health Insurance Portability and Accountability Act (HIPAA). The following changes were incorporated into the template to align disclosure prompts with leading-edge regulatory developments:

- Substitute "personally identifiable information" with "personal information" adapted from the definition under the California Consumer Privacy Act of 2018.[91]
- Substitute "protected health information" with "consumer health data" adapted from Washington state's My Health My Data law of 2023.[92]

These substitutions are more than nominal; they are design choices that have their own tradeoffs. The primary reason for choosing regulatory references from California and Washington was to select categories that large numbers of companies are already tracking or will need to track soon.

88 Sustainability Accounting Standards Board, Health Care Delivery Sustainability Accounting Standard, 2018, HC-DY-230a.3, p. 16.
89 Sustainability Accounting Standards Board, Health Care Delivery Sustainability Accounting Standard, 2018, HC-DY-230a.3, p. 16.
90 Sustainability Accounting Standards Board, Drug Retailers Sustainability Accounting Standard, 2018, HC-DR-230a.1, p. 10.
91 The California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020, represents a significant leap in privacy legislation, and the core of the change is an expansive concept of personal information. Lydia de la Torre, "What is 'Personal Information' under CCPA?" California Lawyers Association, accessed June 12, 2023, https://calawyers.org/antitrust-unfair-competition-law/what-is-personal-information-under-the-california-consumer-privacy-act/.
92 Washington's My Health My Data law, which goes into effect in 2024, reflects recent trends in other U.S. states which aim to provide more data privacy protections for health-related data outside the scope of HIPAA. Amy Olivero and Anokhy Desai, "Washington's My Health, My Data Act," International Association of Privacy Professionals (updated April 2023), https://iapp.org/resources/article/washington-my-health-my-data-act-overview/.

Consolidation

To improve coherence and brevity, we consolidated two similar disclosures that our panel of experts identified as critical during the study. The single remaining disclosure is D1, which is identical with what panelists saw during the study: "Disclose a privacy and/or data protection policy that covers the organization's entire operations, including third parties." The similar but slightly different disclosure that we omitted from the final list and template was "Disclose the organization's policies or commitments regarding customer privacy."

Appendix B: Abbreviations

CLTC Center for Long-Term Cybersecurity

EOS EOS at Federated Hermes

ESG Environmental, Social, Governance

FTC U.S. Federal Trade Commission

GDPR The European Union's General Data Protection Regulation

GRI Global Reporting Initiative

PRI U.N. Principles for Responsible Investment

RDR Ranking Digital Rights

SASB Sustainability Accounting Standards Board

SEC U.S. Securities and Exchange Commission

WBA World Benchmarking Alliance

WEF World Economic Forum

Appendix C: Experimental Disclosures

This Delphi study asked participants to respond to 14 experimental disclosures, in addition to 73 disclosures derived from extant sources in industry, civil society, and standard-setting literatures. Although the experimental prompts sought to address some known problems in nonfinancial reporting (such as inadequate quantitative metrics) and some trending topics in policymaking (such as secure software development), none of them reached the critical threshold (>60 percent) during the survey rounds.

The researcher created the following 14 experimental disclosures, which are based on a combination of desk research and background interviews completed prior to this study. Presented below each are the percentage of panelists who rated the disclosure as critical and the relevant survey round(s).

DATA GOVERNANCE

1. Disclose the number of data protection impact assessments that led to stoppage of design, development, or deployment of a product or service.
   <40 percent round 1

CYBERSECURITY

2. Disclose to whom the CISO (or equivalent) reports.
   <40 percent round 1
3. Disclose the subject matter of cybersecurity training modules.
   <40 percent round 1
4. Disclose the percentage of the organization's workforce that has completed cybersecurity training modules.
   <40 percent round 1
5. Disclose how the organization incentivizes good cybersecurity hygiene in its workforce.
   <40 percent round 1

6. Disclose the number of scenario-based testing exercises the organization has conducted.
   <40 percent round 1
7. Disclose the number of security findings that the organization triaged.
   <40 percent round 1
8. Disclose the number of security flaws discovered that led to stoppage of design, development, or deployment of a product or service.
   <40 percent round 1
9. Disclose the number of security findings discovered that led to triage of design, development, or deployment of a product or service.
   <40 percent round 1
10. Disclose how the organization meets industry best practices for secure software development [such as using Open Source Security Foundation Scorecards or the NIST Secure Software Development Framework].
    40–60 percent round 1, <50 percent round 2
11. Disclose how the organization contributes to the sustainability of open source software communities.
    <40 percent round 1

ARTIFICIAL INTELLIGENCE

12. Disclose the number of algorithmic impact assessments that led to stoppage of design, development, or deployment of a product or service.
    <40 percent round 1
13. Disclose the percent of vendors the organization engages for vendor risk assessment for algorithmic systems.
    <50 percent round 2
14. Disclose the number of vendors dropped because of inadequate performance on risk assessment for algorithmic systems.
    <50 percent round 2

About the Author

Dr. Jordan Famularo is a postdoctoral scholar at the University of California, Berkeley's Center for Long-Term Cybersecurity, where she leads research to explore how norms evolve in communication between companies and their stakeholders with respect to corporate responsibility, risks, and opportunities inherent in their data practices and digital technologies. Her culture- and communication-based research develops new approaches to communicating and accounting for digital harms, and suggests solutions that amplify the benefits of good data practices. She also produces collaborative, multidisciplinary research on dataset development ethics for artificial intelligence and machine learning, which has been presented at the Conference on Computer Vision and Pattern Recognition and the Conference on Neural Information Processing Systems. Previously, Jordan was Theodore Rousseau Fellow at New York University's Institute of Fine Arts.

Acknowledgments

The author extends special thanks to the Delphi study participants and four external project advisors: Eric Meerkamper, for guidance on methodology; Diana Glassman and Navishka Pandit, for institutional investor perspectives; and Jayant Narayan, for assistance with scope and recruitment. At CLTC, Chuck Kapelke and Ann Cleaveland provided valuable editorial support, and Hanlin Li and Jessica Newman provided input on a draft. The author thanks Nicole Hayward for her talent with design and production.

Cite as:

Famularo, Jordan. *A Template for Voluntary Corporate Reporting on Data Governance, Cybersecurity, and AI: Designed for the Mobile Health Market*, Center for Long-Term Cybersecurity, University of California, Berkeley. August 2023, https://cltc.berkeley.edu/publication/corporate-reporting-template.

We thank Omidyar Network for generous support of this project.