ACXIOM HEALTH

OUR COMPREHENSIVE APPROACH TO CONSUMER PRIVACY AND ETHICAL DATA USE

A MODEL FOR HEALTH: PRIORITIZING PRIVACY

Patient-centered payers, providers, and pharmaceutical and life sciences firms focus on fostering proactive and productive conversations between people and their healthcare providers. Acxiom partners with these organizations to help them better understand and connect healthcare professionals and patients with timely and relevant information on medical breakthroughs and therapies to support informed health decisions and improve outcomes.

To protect patient and consumer privacy, Acxiom adheres to all Health Insurance Portability and Accountability Act (HIPAA) compliance standards, ensuring we do not collect, license, or use any HIPAA-regulated protected health information (PHI). Instead, we use our proprietary data and a health-related data set comprised of surveys, claims information, and electronic health records (EHR) ethically sourced from trusted and credentialed third-party partners. This information comes to Acxiom in a de-identified state according to HIPAA regulations. In other words, this data arrives at Acxiom without access to PHI or personally identifiable information (PII), guaranteeing consumer privacy.

We use this de-identified data set to create “look-alike” models to help healthcare organizations predict interest in information about conditions, treatments and products, or services, identify and engage potential customers, and communicate personalized messages that could improve the consumer experience.

Before entering the modeling process, Acxiom’s health-related data is tokenized per HIPAA de-identification regulations, replacing any personal identifiers with encrypted tokens to prevent re-identification and ensuring the resulting models meet trade industry regulations. Additionally, our health data process, environment, and access protocols regularly undergo independent validation assessments to confirm HIPAA compliance.

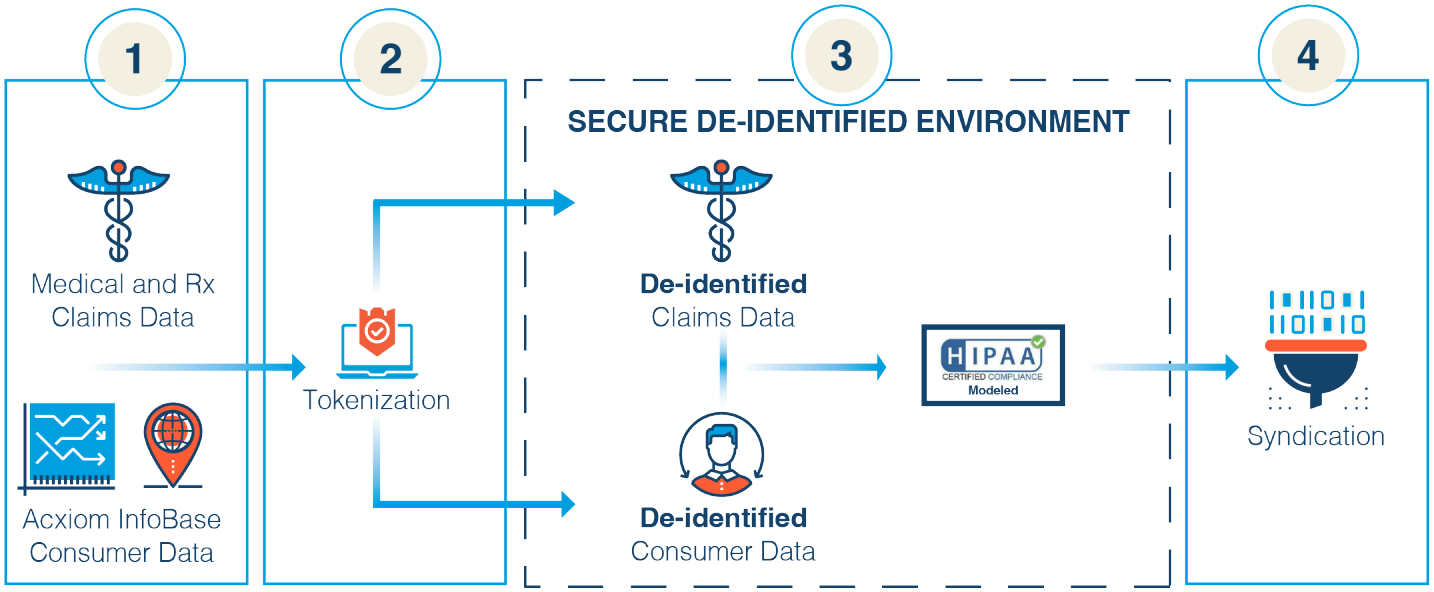
To safeguard against potential harm to consumers and our clients, Acxiom classifies each look-alike model with a privacy classification prior to development:

- **Generally Available Models:** Low risk of harm, available for general use.
- **Restricted Models–Whitelisted:** Elevated potential risk for harm requiring a Privacy Impact Assessment (PIA) prior to client use.
- **Restricted Models:** Higher risk for harm, requiring a PIA each time a client expresses interest in using the model, especially those concerning interest in information about mental or sexual health, and involves submission and review of FDA-approved marketing materials to ensure compliance and mitigate risks.

Acxiom is deeply committed to ethical data practices and safeguarding an individual's privacy. We do not collect or license PII associated with reproductive health or sexual orientation. Acxiom also avoids collecting information about visits to, and tracking movements between, sensitive geographical locations like medical clinics, addiction treatment facilities, places of worship, and schools. We do not gather detailed transaction data that could be used to identify a person's specific transactions or purchases at a granular level, such as medication. Importantly, we do not license our data products to law enforcement. Furthermore, Acxiom has protective measures in place to prevent our data from being misused in unfair discriminatory ways, including rate setting or coverage denial based on pre-existing conditions.

We set a high bar for responsible data use, going beyond what the law requires to ensure we operate in ways that are just and fair to people—and we expect the same from our clients and partners.

MODELING PROCESS ENSURES HIPPA AND NAI COMPLIANCE



A LEGACY OF TRUST

Since 1969, Acxiom has been a pioneer in data privacy and ethics, dedicated to transparency, access, and consumer choice. Our privacy framework is built on these principles, guiding how we collect, use, and share data. We have led the industry in responsible and ethical data practices for over half a century, appointing the first chief privacy officer, ensuring consumer opt-outs, protecting personal information, and upholding fair information practices.

We are engaged members of major trade associations and adhere to their self-regulatory guidelines. Our team of U.S. and global privacy experts actively monitors and ensures compliance with key laws and regulations, including the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and HIPAA.

Recognized for our expertise, we frequently advise leaders across regulated industries, offering guidance on the nuances of current and emerging legislation. Additionally, we regularly contribute to public and policymaker discourse on the intersection of consumer data, marketing, and the internet while advocating for a balanced national law that protects consumer privacy without stifling innovation.

EXPERTS AT KEEPING DATA SECURE

In addition to our comprehensive privacy practice, Acxiom has rigorous administrative, technical, and physical safeguards to protect the data we collect, process, and use, mitigating the risk of unauthorized access. We hold numerous security certifications and undergo regular independent third-party audits, ensuring our practices meet the data security and customer data protection standards.

We also enforce our data security policies by carefully screening our suppliers and clients. Acxiom conducts over 500 Privacy/Data Protection Impact Assessments annually, examining our products, data sources, client processes, and the code we write to process data.

HITRUST CSF Certified | ISO 27001 | NIST Cybersecurity Framework | AICPA SOC SOC 2 TYPE II

- Industry's First Chief Privacy Officer (CPO)
- Modeling output in accordance with Network Advertising Initiative (NAI) guidelines
- Expertise in navigating state and federal regulations
- Rigorous ecosystem ethical standards
- Data processes, environments, and access protocols regularly validated by independent third parties for HIPAA compliance

IMPORTANT INFORMATION

Acxiom's models do not predict whether a particular individual has a past, present, or future physical, mental, or medical condition. Clients may not use our models in a manner that would express or imply a consumer may have a past, present, or future physical, mental, or medical condition.

FOR MORE INFORMATION

about our privacy practices, please visit our privacy center or contact us at info@acxiom.com.

ACXIOM

©2024 Acxiom LLC. All rights reserved. Acxiom is a registered trademark of Acxiom LLC.

GLOSSARY OF KEY TERMS

CLAIMS DATA The information gathered from healthcare billing, encompassing patient demographics, diagnoses, treatments, provider details, and service costs. Our data supplier de-identifies the data in accordance with HIPAA regulations and guidelines before delivery to protect consumers' privacy.

DE-IDENTIFIED DATA Information that has had all personal identifiers removed in accordance with state and federal law, which could be used to trace the data back to an individual. This process protects consumer privacy.

LOOK-ALIKE MODEL A data-driven statistical tool used in marketing to predict the likelihood of customer actions, like identifying an interest in information, based on historical data and behavior patterns, helping businesses improve marketing efforts and make informed decisions.

NETWORK ADVERTISING INITIATIVE (NAI) A self-regulatory association dedicated to responsible data collection and its use for digital advertising.

PERSONALLY IDENTIFIABLE INFORMATION (PII) Any data that could potentially be used to identify a specific individual, either on its own or when combined with other relevant information, including a full name, Social Security number, driver's license number, bank account numbers, passport number, email addresses, or any unique personal identifier.

PRIVACY/DATA PROTECTION IMPACT ASSESSMENTS Processes to identify and minimize data protection risks in projects, involving the evaluation of processing operations, necessity, risk identification, mitigation measures, and stakeholder consultation, crucial for ensuring compliance with data protection laws.

PROTECTED HEALTH INFORMATION (PHI) Any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

TOKENIZATION A data security process where a data element, such as a name or an account number, is replaced with a unique identifier known as a token. This token can be used in a database or system without exposing the underlying data to identification or re-identification by third parties.