Data & Feature Summary

Our model uses data collected from previous customers, referred to as data generators as well, to calculate the probability of filing a claim and the predicted cost of the claim using classification and regression models. The data contains information about their identity such as age, gender, and marital status, their family information like the number of children they have, their socio-economic data (income, home value, etc.), vehicular information and data on their past claims.

When preprocessing the data, we remove sensitive information (which can lead to biased predictions or privacy violations) about the customers such as the number of children, the value of their home, their income, parental & marital status, gender, education, and occupation. We have only used the top 10 important features in our model, and from this, we have excluded the features tagged as sensitive.

Ethical Challenges

In developing our insurance claim prediction models, we face several ethical challenges regarding customer data. Our models require sensitive information including identity details, family information, socioeconomic status, behavioral history, and vehicle information.

From a deontological perspective, we must consider issues of consent, as customers typically provide data for insurance services, not specifically for AI model training. This raises questions about whether blanket consent for "research and product development" is sufficient or if more specific, informed consent is required. There's significant ambiguity about whether individuals maintain rights over their data after sharing it with our company. Frameworks like GDPR[4] suggest individuals retain certain rights over their identity-related information, but the extent of these rights in AI training contexts remains contested. Using sensitive personal information (such as income, family composition, or behavioral history) must be balanced against preserving human dignity, particularly when these attributes influence insurance decisions that could significantly impact customers' financial situations.

From a utilitarian approach, we recognize that some data could perpetuate historical biases in insurance pricing if used inappropriately. Historical claim data might reflect systemic disparities in claim processing or reporting, potentially leading to discriminatory outcomes when used for prediction. Different data types carry varying levels of sensitivity and potential for harm - vehicle information might be less sensitive than income data, but both influence predictions. The tension between improved insurance modeling benefits (more accurate pricing, better risk assessment, potential cost savings for low-risk customers) and individual privacy rights remains central. While better models could benefit the broader customer base, this must be weighed against privacy concerns.

These ethical challenges require us to develop thoughtful policies that respect individual rights while enabling beneficial innovation. Any approach must balance multiple stakeholders' interests, including customers, regulators, and the company itself while adhering to both legal requirements and ethical principles that may sometimes extend beyond what the law strictly requires.

Proposed Standard

We propose Tiered Consent with Transparency and Purpose Limitation standards for our data collection practices. This approach separates basic insurance service data (required) from research and model development data (opt-in). For model development, we will request separate, explicit consent with plain language explanations, specification of included attributes, and clarification that individual data cannot be fully removed once incorporated into training models.

Our standard emphasizes data minimization by only collecting information with demonstrable relevance to insurance risk. We will establish clear retention periods with subsequent anonymization of personally identifiable information. To maintain transparency, we will issue regular reports showing which data categories influence our predictions.

This standard is ethically permissible because it respects individual autonomy through meaningful consent, minimizes potential harm through purpose limitation, creates transparency around data usage, and balances individual rights with collective benefits while enabling valuable model development. It acknowledges both rights-based and consequence-based ethical frameworks, providing a balanced approach to the complex challenge of using personal data in predictive insurance models.

Potential Objections & Future Solutions

We recognize that using the customer's data for training and building AI modes can raise ethical and legal considerations. While we do not believe that the data generators maintain complete ownership over the results and insights we have derived from the models, we are committed to respecting their privacy and ensuring responsible data usage.

There may be an occurrence where customers may request that their data be removed from the model (post-consent withdrawal). However, we acknowledge that removing individual data points from a large model is practically infeasible. In such cases, we can ensure that the customer data will be stored on the model's server only for the required period of time and will be anonymized or deleted from the server post the time period. We can also enable the customer to remove their data from any future use and product development, should they wish for it - under CCPA[1] and CPRA[2], customers can request their data to be removed, but this does not extend to already-trained models. Another concern that the company may face is that the data generators may later claim they misunderstood how their data would be used, leading to disputes. We can address this by using plain, clear language statements and visual aids to explain the data usage. This will allow the customers to opt in or opt out of the development processes - under CPRA[3] and GDPR[4], consent must be "freely given, specific, informed and unambiguous".

Customers may object to the collection of their data if they feel that it is irrelevant, such as the number of dependents, their parental status, or the color of their car. In such cases, we can share the categories/features that we will be using in specific models and how that feature may be relevant - under CCPA[5], data collection should be limited to necessary purposes only. This will help to foster trust as well.

There may be a distrust in the data generators due to the opacity of the details of the model, especially when it's regarding the claim costs. We can provide simplified insights to the customers, such as your probability of claim is predicted to be high due to a history of accidents - under CPRA[6], individuals have the right to give meaningful information on automated decisions. We can also use explainable AI such as LIME to help customers understand the interpretation of the results.

However, we will have to be careful in finding the trade-off line of how much information to divulge to the data generators so that any sensitive data about the company is not at risk. The complete ownership of the results lies with the company and while we try to quench questions about the data usage and practices to the best of our ability, we will ensure that company data will not be at risk of exposure. This approach will address possible objects while ensuring transparent and legally compliant data practices.

References:

[1] California Consumer Privacy Act, California Civil Code Section 1798.100 et seq., 2018.

[2] California Privacy Rights Act, California Civil Code Section 1798.100 et seq., 2020.

[3] California Privacy Rights Act, California Civil Code Section 1798.120, 2020.

[4] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 32.

[5] California Consumer Privacy Act, California Civil Code Section 1798.100(b), 2018.

[6] California Privacy Rights Act, California Civil Code Section 1798.121, 2020.