RMEx - What compliance means to us

Compliance means many things to many people. In our case, we believe that compliance has to be all encompassing. There is a simple reason for this. There is usually zero tolerance when it comes to compliance failures. There is no grading and no gray area. You pass or you fail. Unfortunately, compliance can not be targeted in small projects. You may be penalized for calling a cell phone after 3 months, when the real problem was created at the time the account was loaded. It is therefore important to understand where the dots are, and how they should be connected.

This document attempts to provide some mid-level detail on RMEx's compliance features. With this knowledge, you should be able to select specific areas to review in more detail, within other areas of our documentation.

We will present our compliance features in 3 sections - Security features, dialers and legislation. This separation may help to clarify this area of collections that has become increasing complex over the last few years.

Table of contents

You can click on a topic to go to a specific area.

SECURITY FEATURES

Security features deal with access to features and data. Most collection companies share resources across multiple projects. Some larger clients will insist that only designated people work their accounts. Access to data must also be restricted based on an individual's role within the company. Some states require that a collector is licensed in that state before they are allowed to work accounts that originate in that state. Information that could be used to steal identities or access financial data must be protected.

All of these requirements can be met with well-designed software. The following section presents some of the key security features of our system.

Limiting access by role and responsibility

When a user is set up in RMEx, you can indicate the different areas and sections of the tree menu (menus) they can access. 

- Some example of areas that can be defined are Security, Client updates, Client inquiry, Payment entry and Month-end processing
- Some example of menu options are Management, Payments, Daily reports and Periodic reports
- Users can be restricted from accessing medical or bankruptcy information
- Some users can be set up to view but not change account information. A person who enters returned mail does not need to view client or patient information!
- By using special description codes, users can be stopped from accessing selected accounts. This option is set up on the system control file for "Description Codes" (Special warning message - User will need special authority for access) and can be overridden using the option "Allow access-special desc.code (Y)" on the System Security
- On System Security, the feature "Hide client, patient, notes (Y)" allows role-based access to information that may be considered private

Access to clients can be controlled at user level

Depending on your client base, you may run into situations when a large client insists that only a few specific agents are allowed to work and view their accounts. 

- You can set up client codes or client group codes that access should be allowed or restricted, based on User ID
- Clients can be grouped in “Profile codes”. Instead of keying in many different client or group codes for a User ID, you could specify “CABLE” to refer to all Cable TV clients, as an example.
- Major options and programs run by each user, are tracked. From the Management Menu, and the “Smart Code/User Audit Options”, the “User Activity inquiry” will display options run by a user for a selected period.

States that require licensing of agents

Some states require agents to obtain a special license before they can work a consumer based in their state. In these instances, access must be limited based on User ID and the state on the account. These rules can be set up within System Security. 

Making sure you are talking to the correct consumer

Privacy of the consumer and their data is very important. Can you ever ensure that you are talking to the correct consumer? Can you tell a client that consumer information is secure and can not be viewed by anyone other than an agent who we know is talking to the right consumer? Yes! What if we did not allow an agent to view account details until the consumer had provided sufficient information to be authenticated by the system? 

- The “right party authentication options” are set up from within System Security
- The feature is set up for specific clients
- You can select the authentication options from full SS#, last 4 of SS#, full DOB, month and year of DOB, address information, full client account number or last 4 of client account number
- You define the minimum number of items that must be matched to authenticate the consumer
- Successful authentication, or the failure to authenticate the consumer are logged using smart codes

- If authentication fails, the account can be transferred to a manager or supervisor for manual verification. Once this is done the agent can work the account without the normal verification process

Auditing and tracking changes made by an agent

Knowing who accessed an account, and what information was updated is important. RMEx will document important changes made, within the account notes or the audit notes. 

- Changes to key account information (e.g. phone numbers, addresses) are documented. The old information is saved in the notes
- Information such as a new payment arrangement or promise, are also documented by the system
- When close codes, owners or worker codes are changed, these changes are documented
- There is an option to document an account when a user views an account, but does not do anything to indicate that they accessed the account
- The extreme case where a user viewed an account, and exited abnormally by “closing the window” is also addressed! An abnormal exit is also documented in the notes, along with the User ID
- Notes can be searched based on selected words or phrases

Securing key financial data and socials

Social security numbers, checking account and credit card information is very important. This is sometimes the case with client account numbers, which may contain active credit card numbers. This information has to be securely stored and only viewed by those who should have access to the information.

- All socials are encrypted at rest, using advanced and accepted standards of encryption
- Credit card information is encrypted. Optionally, you can work with a company to process your credit cards, and use “tokens” instead of storing card information on your system
- Checking account information is encrypted
- Depending on how users are set up, information can be masked, so full socials, credit card or checking account information is never displayed
- There are 3rd party products and hardware solutions to encrypt data backups 

How secure is your hardware platform?

Everyone is aware of the vulnerabilities of PC platforms and the related system software. Our hardware platform, the IBM i5 (formerly known as the AS/400 and iSeries) offers the highest levels of system security. This platform has been awarded a C2 rating for security. C2 is a security standard defined by the U.S. government in the Department of Defense Trusted System Evaluation Criteria.

ISSUES RELATED TO DIALERS

Dialers offer great efficiencies, with the ability to quickly work through very high volumes of phone numbers. If dialers are not properly managed, they lead to complaints and the violation of some basic rules. A majority of the complaints about dialers relate to nuisance calls (canceling calls before the consumer is able to get the to the phone, or dead air when the call is picked up), calling outside of the permitted hours or calling cell phones if they should not be called. This section describes some of the features that help you to manage these complex requirements.

Abandoned calls

Although there has not been much focus on the area of abandoned calls within collections, it is often referenced in guidelines discussed by states or federal agencies.

RMEx's integrated dialer will offer the following features :

- Calls will not be canceled by the dialer. The phone is always rung the specified number of times
- Dead air is minimized because the dialer does not use traditional pacing methods
- Abandoned rate is managed by the dialer and not by supervisors who can change the pacing of the dialer

Calculating the allowed calling period

Many dialer companies will tell you that their dialer handles time-zone management, ensuring that consumers are always attempted within the legally allowed calling times. The reality is that a dialer can not accurately determine the allowed calling period. There is a great deal of information that is required to correctly calculate the allowed calling period for a given phone number!

RMEx considers the following when allowed calling period is computed.

- Current tables of time-zone codes for different areas and phone numbers are utilized in the calculations. This information is licensed through one of the leading providers of global contact data quality tools
- All the active numbers on a consumer's account can be considered, including phone numbers on linked accounts (we will look up numbers on the account detail screen as well as active numbers in the other phones window)
- The consumer's state is considered
- Toll-free numbers are considered. They can also be ignored
- For a most conservative approach, telephone exchange and zip code can be considered
- Daylight savings time is factored into our calculations
- State rules can limit IVR calls to certain hours in the day
- Predictive calls can be controlled and limited to certain hours
- The most conservative approach can be overridden in many cases, giving users the flexibility to take risks they may choose to
- Numbers that should not be called at the current time can be masked, to stop enthusiastic agents from using a desk phone to place a call

Managing cell phones

Calling cell phones has become an important compliance hurdle. We offer the following :

- Cell phones can be identified and managed *in real time*. You will need to obtain proprietary cell block and ported number information
- Permission to call cell phones can be obtained and notated against the number. Predictive and preview calls can be restricted to cell phones with or without prior permission to call
- The Right Party Contact console will automatically call all numbers, regardless of the type of number (home, work, cell or third party). Different numbers will be dialed *the same number of times*, with each attempt being made at *a different time in the day*. Cell phones will automatically and

dynamically moved to different campaigns so they can be attempted in a preview campaign if required
- You can stop cell phones from being dialed predictively

“Do not call numbers”

Do not call numbers can be set up at the company level. The system will enforce these rules. If a consumer says you should not call a specific number, this number can be disabled, or the phone code changed, and the phone code omitted from certain campaigns.

Inconvenient times to call

If a consumer specifies that you should not call at certain times on certain days of the week, this information can be set up on the account. Our strategy is for you to move these accounts into a different area (QCat) and have these accounts worked through preview mode, where the rules will be enforced.

LEGISLATION

Legislation, litigation and sometimes common sense, will often drive the behavior within a collection operation.

RMEx considers the following in its compliance strategy.

- We handle state licensing requirements. If a company does not have a license to work in certain states, accounts received for those states can be handled in many ways. E.g. they can be closed, forwarded etc.
- The system can ensure that the validation notice is sent out after an attempt or contact. This allows accounts to be worked prior to sending the validation notice
- Many states and cities have rules for call frequency for a single day, or longer periods of time. The system can be set up to define “max calls” and messages at the client, state and city levels. Defaults can be set for the company.
- Attempts, messages and contacts can be separately counted
- You can define a demand letter as an attempt, or treat a message as a contact
- If clients insist that cell phones should not be called using a dialer, we can make sure these numbers are not called through the dialer. We have

methods of counting and tracking a cell phone call that is manually placed through a desk phone!.

- In the event of a disaster, phone calls and letters can be stopped for a state or a group of area codes
- Sometimes you are required to warn a consumer that the call is being recorded. The agent can be reminded of this based on the consumer's state
- Some states require that if a home and work number exist, the home number be attempted and the work number tried only a given number of days later. We systemically manage this rule on the States System Control file. If the rule applies and there is a work number, it will be masked until the work number can be called
- Third party numbers can automatically be disabled after a certain number of attempts or contacts. These rules are set up at the "Phone codes" level
- Predictive or preview calls (autodialer calls) to *any* number can be stopped at the state level.
- Some cities require that the details of a payment arrangement be printed on a notice. We can print the details of the arrangement (installments and due dates) regardless of the number of installments
- States have strict rules about the length of time you are allowed to work an account. These complex rules can often get you in trouble if you continue to work an account after you are supposed to cease efforts based on the statute. With RMEx, you set up the statute and rules (at the state level) and walk away. Accounts will get closed automatically, on the exact date specified in the rules.

Summary

The above information should give you a good idea of how we have incorporated security, privacy laws, dialer controls, cell phone management, state and city rules and well as many other "common-sense" standards into our compliance strategy. Unfortunately, this is not a simple area to administer. The complete landscape is quite vast, and while RMEx allows you to do a great deal with no custom programming, you have the burden of mastering the features and options that make RMEx so powerful.

Quantrax CORPORATION | RMEx Receivables Management Expert