U.S. Regulations & Compliance for Church Phone Systems

By ClearlyIP Published May 12, 2025 65 min read

Regulations and Compliance for Church Phone Systems (U.S.)

1. Overview of Phone Systems Used in Churches

Churches utilize a range of telephone systems depending on their size and needs. Common setups include traditional landlines, on-premises PBX systems, and modern VoIP/ cloud solutions:

- **Plain Old Telephone Service (Landlines):** Many smaller churches rely on standard analog landline phones provided by local carriers. Landlines are simple and reliable, but offer limited features. They typically support basic voice calls and voicemail. Regulatory-wise, they are subject to telephone utility rules but generally straightforward to manage.

- **Private Branch Exchange (PBX) Systems:** Larger churches or multi-building campuses may use a PBX – an internal phone switching system. Older PBXs were hardware-based (using onsite switchboards), while newer ones are IP-PBX systems running on servers. A PBX lets staff call each other by extension, share outside lines, and set up call routing (e.g. an auto-attendant). PBXs offer control and advanced features, but require maintenance. If a church has multiple offices or a school, a PBX can integrate them but must be configured to comply with dialing and 911 rules (see §2).

- **VoIP (Voice over IP) Phone Systems:** VoIP transmits calls over the internet instead of traditional phone lines. Many churches are adopting VoIP for cost savings and flexibility. For example, Central Baptist Church in Illinois moved to a cloud VoIP service to unify staff across two campuses and support mobile staff working off-site (Source: onsip.com). VoIP systems can be on-premises (an IP-PBX server) or hosted by a provider (cloud PBX). They offer features like automated attendants, voicemail-to-email, conferencing, and easy scaling. However, VoIP phones require a stable internet connection and proper E911 configuration (since location is not fixed).

- **Cloud-Based/Hosted Phone Services:** These are essentially VoIP services managed by vendors (e.g. RingCentral, OnSIP, Ooma, etc.) and delivered from the cloud. Churches opt for hosted PBX to avoid maintaining hardware. Handsets or apps connect to the provider over the internet. Cloud phone services are typically subscription-based and include features like call routing, IVR menus ("press 1 for office"), call recording, and integration with mobile phones. The provider handles updates and regulatory features (such as 911 routing), but the church must input correct location data and adhere to usage rules. Hosted systems are popular with churches because they can be cost-effective and allow staff to use softphone apps on laptops or smartphones (Source: onsip.com).

Each type of system comes with compliance considerations. For instance, any multi-line system (whether a PBX or VoIP) must support direct 911 dialing under federal law, and VoIP services must provide Enhanced 911 (E911) functionality (discussed below). In the following sections, we explore the regulatory landscape affecting these phone systems in U.S. churches.

2. Regulatory Landscape for Church Phone Systems

Churches, though typically non-profit, are not exempt from telecommunications regulations. They must navigate a patchwork of federal, state, and local rules that govern telephone systems. Key areas of regulation include FCC rules, emergency 911 requirements, call recording laws, accessibility mandates, and even tax considerations:

2.1 Federal Communications Commission (FCC) Regulations

FCC Oversight: The FCC regulates interstate and international communications, and many of its rules apply to phone services used by churches. Even though a church is not a commercial carrier, using phone services ties it to FCC mandates (often implemented via the service providers or equipment). Some of the most pertinent federal regulations include:

- **Enhanced 911 (E911) and Multi-Line Telephone Systems:** The FCC enforces federal laws (Kari's Law and Section 506 of RAY BAUM's Act) to ensure people can reach emergency services and be located easily. Effective February 2020, Kari's Law requires that anyone must be able to dial 911 directly on multi-line systems **without** needing to dial an access code (no more dialing "9" for an outside line)911.gov. It also requires that the phone system *automatically sends a notification* to a designated staff or security location when a 911 call is made, including callback number and caller location details911.gov. RAY BAUM's Act, implemented via FCC rules starting 2021, mandates that 911 calls convey a **"dispatchable location,"** meaning the street address *plus specific location info* (building, floor, room, etc.) to help responders find the caller911.gov. These rules apply to any enterprise using an MLTS (Multi-Line Telephone System), which would include a church's PBX or VoIP system911.gov. In short, new phone systems must be configured to enable direct 911 dialing and transmit location info for emergency calls, or the church could face compliance issues or liability.

- **Interconnected VoIP Services:** If a church uses an interconnected VoIP phone service (able to reach the PSTN), FCC regulations require that service to provide E911 as a standard feature (Source: tap.gallaudet.edu)(Source: tap.gallaudet.edu). The church must register an emergency location with the provider and keep it updated. Providers must route 911 calls to local emergency centers and pass along the caller's number and registered address (Source: tap.gallaudet.edu). This means that if a church moves or uses a cloud phone at a new site, it has a duty (often via the provider's interface) to update the location for 911 purposes.

- **Telephone Consumer Protection Act (TCPA) & Robocall Rules:** Churches occasionally use mass calling or texting—for example, automated calls for event announcements, prayer chains, or fundraising. These practices fall under the TCPA, enforced by the FCC. Nonprofits historically had some exemptions (especially for calls to landlines), but recent rule changes in July 2023 narrowed those exemptions (Source: churchlawcenter.com). Under revised FCC rules (pursuant to the TRACED Act), tax-exempt nonprofits may make only **three** artificial/prerecorded voice calls to any residential number within a 30-day period *without prior consent* (Source: churchlawcenter.com). Previously, nonprofits could make unlimited robocalls to residential lines for non-commercial purposes, but now they face stricter limits (Source: churchlawcenter.com) (Source: churchlawcenter.com). Calls or texts to cell phones using an autodialer or prerecorded message still generally require the called party's consent under TCPA (the 2023 FCC changes left wireless rules unchanged (Source: churchlawcenter.com)). In practice, if a church or its vendor uses automated dialing to reach congregants, it must ensure compliance – e.g. obtaining consent for automated texts, limiting the volume of robocalls, honoring opt-outs, and avoiding calling numbers on the National Do-Not-Call Registry (though purely informational or fund-raising calls by charities may be exempt from *DNC* rules, they still must meet the new volume limits for prerecorded calls).

- **FCC Equipment Standards:** All telephone equipment used must be FCC-approved for connection to the network. This is usually handled by the manufacturer; churches should buy FCC-certified phones (most standard phones sold in the U.S. comply with Part 68 and other rules). Additionally, FCC rules require phones in certain contexts to meet **Hearing Aid Compatibility (HAC)** standards. In fact, federal law (the Hearing Aid Compatibility Act of 1988) requires that all telephones (including cell phones) be compatible with hearing aids (Source: healthyhearing.com). Thus, any new desk phone or cordless phone a church deploys should be HAC-compliant (most are, as per FCC mandate).

- **Privacy of Communications:** While not a rule the church enforces, it's worth noting the **Electronic Communications Privacy Act** (a federal wiretap law) prohibits intercepting phone calls. There is a *business use exemption* that lets employers monitor calls on equipment they provide **if done in the ordinary course of business** (Source: churchlawandtax.com). For a church, this means if you have a call recording system or listen in on calls for quality or security, it should be limited to church-related calls. Personal calls of employees or congregants should not be monitored without consent, or the church could violate federal law. We discuss call recording laws in detail later (see §2.4).

In summary, FCC regulations set the baseline: ensure 911 can be dialed and locatable, respect telemarketing and anti-robocall rules even as a nonprofit, use compliant equipment, and handle any call monitoring cautiously within legal bounds.

2.2 State and Local Telecom Compliance

Beyond federal rules, churches must consider state and local regulations which can vary widely:

- **State Public Utility Commissions (PUCs):** Many states regulate telephone services and may impose their own requirements. For instance, some states passed their own versions of Kari's Law or E911 mandates before the federal law took effect. By 2020, at least 24 states had enacted legislation on MLTS 911 dialing and location obligations for organizations above certain sizes or when installing new phone systems (Source: 911.gov). For example, Maryland's law (H.B. 1080, effective 2017) required that MLTS allow direct 911 dialing and provide callback number and address to 911 (Source: intrado.com). Texas implemented a state Kari's Law in 2015 after a high-profile incident, and Illinois, Colorado, Tennessee, and others also have state-specific E911 rules for businesses and institutions. Although the federal Kari's Law/RAY BAUM's Act now covers the basics nationwide, churches should be aware of any additional **state-level requirements** – e.g. some states mandate **notifications to onsite personnel** or registration of MLTS with the local 911 authority. California, as another example, requires businesses to maintain accurate 911 location info in the 911 database and directed carriers to educate MLTS customers on their responsibilities (Source: cpuc.ca.gov)(Source: cpuc.ca.gov).

- **Local Building Codes & Emergency Ordinances:** In some localities, building or fire codes require certain phone capabilities. A municipality might require that any place of assembly (which could include a large church or religious school) have at least one accessible telephone line for emergency use. Alaska's state law even allows municipalities to **require** MLTS operators to provide E911 service (ensuring location info goes to the PSAP) (Source: intrado.com). Large church campuses with elevators or fire alarm systems may need a dedicated landline for those systems (per fire code). It's wise for church facilities managers to check local codes – for example, whether an elevator emergency phone or alarm panel in the church must be connected via a traditional analog line (common requirement), even if the rest of the phones are VoIP.

- **State Call Recording and Privacy Laws:** (Covered in §2.4 below) States govern consent for recording calls, and a church located in a "two-party consent" state must abide by that law when recording conversations, even if federal law is one-party.

- **State-Specific Telecom Fees:** Some states impose 911 fees, service fund fees, or utility taxes on phone lines. These usually appear on the phone bill. While these are paid by the customer (the church), regulations define them. For example, states set monthly 911 surcharge amounts that every line or VoIP number must contribute to fund emergency services. Churches should simply be aware of these fees as a normal part of compliance (and ensure their phone provider is remitting the fees).

In practice, compliance with state/local telecom rules often involves coordination with service providers (who usually incorporate these requirements) and staying informed via state government or denominational resources. Churches undertaking major phone upgrades should check state laws or consult an IT/telecom advisor to ensure all state and local obligations (like MLTS registration or specific notices) are met.

2.3 Emergency Services and E911 Requirements

Emergency Calling Requirements (Kari's Law & RAY BAUM's Act): Perhaps the most critical regulations for any organization's phone system are those ensuring access to 911 and location reporting. Churches, like any other organization, must configure their phone system to comply with these emergency rules:

- **Direct 911 Dialing:** As noted, Kari's Law (47 U.S.C. § 623) requires that from any multi-line telephone (such as an office phone on a PBX or VoIP system), a user can dial "911" without any prefix or code911.gov. This means if your church's phone system currently requires dialing "9" or another number to get an outside line, that must be reconfigured or eliminated for 911 calls – people should *not* have to think about an extra digit in an emergency. This applies to new systems installed after Feb 16, 2020, but practically, **all** existing systems should have been updated if possible. If a legacy system cannot be updated to allow direct 911, it is a serious liability.

- **911 Call Notification:** Kari's Law also mandates that the system send a notification (e.g. an email, text, pop-up, or audible alert) to a designated location *on- or off-site* when someone dials 911911.gov. In a church, this could be set to notify the front office, security team, or certain staff. The notification should include at least the fact that a 911 call was made and a callback number (and ideally info like extension or room). The goal is that someone on-site can meet first responders or assist. For example, if a 911 call comes from a classroom phone in the church's school, an administrator should be alerted to direct paramedics to the right room.

- **Dispatchable Location for 911 (RAY BAUM's Act):** The FCC's rules implementing RAY BAUM's Act took effect starting January 6, 2021 (with phased deadlines through January 2022 for different types of devices). These rules require that any 911 call from a multi-line system delivers a "dispatchable location" to the 911 center – essentially, the *validated street address* plus any necessary info like building number, floor, or room to find the caller911.gov. For fixed phones (like a desk phone in an office), the system should have a static location record (e.g., "123 Church St., Building A, 2nd Floor, Office 210"). For nomadic or softphone devices (e.g., a pastor's laptop softphone that could be used from various locations), the system or user must be able to update the location or at least provide a usable location. **Compliance tip:** Churches using VoIP/hosted systems should work with their provider's E911 tools – you may need to register the address of each phone or set up "zones" for larger campuses. If phones are moved, update the location in the system's database. Many cloud providers now let users or admins enter a new emergency address on the fly for softphones. Ensuring these are in place is both a compliance and safety issue. The CPUC (California) summarized that the new federal rules establish *direct 9-1-1 dialing, notification, and dispatchable location* for outbound 911 in MLTS environments (Source: cpuc.ca.gov) – all three must be met.

- **Testing and Maintenance:** While not explicitly mandated by FCC, it's considered best practice (and sometimes encouraged by local authorities) to periodically test 911 from your system. Coordinate with your local PSAP (911 center) for a non-emergency test call if possible, or use test numbers (some VoIP providers have a 933 test service to read out what location is registered). This helps ensure your church's phones indeed reach the correct 911 center and transmit the correct info. Kari's Law and RAY BAUM's Act violations can result in FCC enforcement action if reported, but more importantly, non-compliance could cost lives or lead to liability. The FCC can issue fines for non-compliant phone system vendors or operators; for instance, businesses have been put on notice to upgrade systems or face penalties (Source: cpuc.ca.gov).

Example Case: The importance of these 911 rules was underscored by the tragedy that inspired Kari's Law: in 2013, a 9-year-old girl in a motel tried repeatedly to dial 911 while her mother was being attacked, but **no calls went through because the motel's phone required dialing "9" first**911.gov. This incident (though not in a church) led to the push for the law. It's a sobering reminder that even a church must ensure anyone – staff, visitors, children – can pick up any phone and reach emergency help without impediment. No one expects an emergency, but preparation is crucial.

E911 for VoIP and Mobile Users: If a church is using solely mobile phones (cell phones) for communications, note that cellular 911 calls rely on wireless carriers' location technology (GPS, network triangulation). Ensure staff know that calling 911 from a cell phone will send whatever location the phone GPS provides – which might be less precise indoors. Some large campuses opt for *Emergency Location Identification Numbers (ELIN)* or dedicated lines to the nearest PSAP. However, for most churches, the key is training and ensuring any VoIP lines are registered. The **National 911 Program** and FCC have released checklists and tools for enterprises to track MLTS compliance911.gov – it may be useful for a church's IT or admin to review those resources.

2.4 Call Recording Laws and Consent Regulations

Churches may sometimes record phone calls – for example, to record incoming prayer line requests, for staff training, or when handling sensitive calls (counseling sessions, etc.). It's **critical** to understand consent laws for call recording, which are primarily governed at the state level:

- **One-Party vs. Two-Party Consent:** U.S. states have different rules on whether you must inform or get consent from call participants before recording. **Federal law (18 U.S.C. § 2511, the Wiretap Act)** sets a baseline of one-party consent – meaning as long as *one party* to the call (for instance, the person doing the recording) consents, it's lawful to record. However, states can impose stricter rules. The majority of states (38 states plus D.C.) follow the one-party consent rule (Source: rev.com). **Eleven states** have "all-party" or "two-party" consent laws, requiring that *everyone* on the call consent to the recording (Source: rev.com). These all-party consent states include **California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, and Washington** (Source: rev.com). (Vermont does not have a specific law and is treated as one-party by default federal law (Source: rev.com).)

- **Implications for Churches:** If your church is in or calling into an all-party consent state, you need to obtain consent before recording. Consent can be explicit (verbal or written agreement) or implied by notification. A common compliant practice is to play a disclaimer at the start of a call: "This call may be recorded for [purpose]." If the person stays on the line after hearing that, it often counts as implied consent in many jurisdictions (Source: mwl-law.com). Churches should implement such measures if, say, they record calls to a counseling hotline or when staff call members and plan to record the conversation. Failing to do so could lead to civil liability or even criminal penalties under state law. For example, a religious organization's contractor was accused of *illegally recording phone calls* with staff without consent in Illinois (an all-party state) (Source: ncronline.org) – highlighting that secret recordings can trigger legal action.

- **Employee Call Monitoring:** If a church monitors or records calls made by its employees (like a church office receptionist's calls), the **business telephone exception** under federal law can apply (Source: churchlawandtax.com). This allows employers to listen in on or record calls *in the ordinary course of business* when using equipment provided by a communications carrier. However, even this has limits: it generally covers **business calls** – if the employee indicates a call is personal, monitoring should cease to avoid violating privacy laws (Source: churchlawandtax.com). The best practice is to have an **internal policy**: inform staff that calls may be monitored or recorded for legitimate reasons, and provide a means for truly personal calls to be made in private.

- **Consent Across State Lines:** If a church staff member in a one-party state calls a congregant in a two-party state (or vice versa), it's safest to assume the stricter rule (all-party) applies. This is a legal gray area, but many organizations adopt the policy of **always disclosing recording** to avoid any dispute. For instance, if a church records prayer line calls and someone from California (all-party state) calls in, the church should have a pre-recorded message or volunteer script to get consent at the outset.

- **Call Recording by Vendors:** Sometimes churches use third-party conference line services or customer management systems that have call recording features. The church is responsible for using those in compliance with the law. Ensure any vendor or software is configured to play the necessary announcements or otherwise allow compliance. Many modern phone systems (cloud PBXs, etc.) have a setting to play a "your call is being recorded" prompt automatically if recording is enabled.

For easy reference, the following table summarizes U.S. call recording consent laws:

CONSENT REQUIREMENT	JURISDICTIONS
All parties must consent (two-party consent law)	11 states: California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, Nevada, New Hampshire, Pennsylvania, Washington (Source: rev.com). (These require every participant's consent; "two-party" effectively means all-party.)
One-party consent (only one participant's consent needed)	39 states + D.C. follow this rule (Source: rev.com). In these states, as long as the church **or** one call participant knows and consents to the recording, it is legal. *(Note: Vermont has no explicit law and is treated as one-party by federal default) (Source: rev.com).*

Practical tip: When in doubt, get consent from all parties. It can be as simple as, "Would you mind if I record this call so I don't miss anything important?" or using an automated disclaimer. This not only keeps you compliant but also builds trust through transparency.

- **Specific Scenarios:** Churches might also need to consider **voicemail recording** – generally, leaving someone a voicemail and recording it on their system is not a two-party issue (the recipient can choose to keep it or not). However, if a church is recording incoming voicemails on a line, that's expected behavior by callers. Another scenario is **recording in-person conversations** (e.g., counseling sessions). That enters a separate area of law, but many state wiretap laws also cover "oral communications" in private. The same consent principles would apply if someone wanted to record an in-person meeting or confession – usually, all-party consent if state law requires. While not exactly "phone system" regulation, it's a related consideration for religious leaders.

2.5 Accessibility and ADA Compliance Issues

Accessibility in communications is an important ethical and legal consideration. Churches serve the public and their members, including those who are deaf, hard of hearing, or have speech or mobility impairments. Several laws and regulations address accessible phone communication:

- **Americans with Disabilities Act (ADA) and Religious Exemption:** It may surprise some to know that **houses of worship are largely exempt from ADA Title III** (the section that requires public accommodations to be accessible) (Source: adata.org). Churches, being religious entities, are not legally required to retrofit buildings or services to ADA standards in the same way a public business must. This means a church might not be *forced* by law to provide, say, a TTY (text telephone) or hearing aid loops under ADA. **However,** many churches voluntarily strive to be welcoming and accessible. Moreover, if the church operates programs not purely religious (like a school open to the public), other laws might kick in. And under ADA Title I (employment), a church with employees may still have to provide reasonable accommodations to disabled employees (though there are some religious exemptions for hiring, disability discrimination law generally applies to employment).

- **Telephone Relay Services (TRS) and 711:** Title IV of the ADA requires nationwide relay services for telephone access by hearing or speech-impaired individuals. This is actually a requirement on telephone companies, funded by telecom fees, ensuring that anyone can dial 711 to reach a relay operator. For a church, the practical point is: be aware of relay calls. If a deaf person uses a relay service to call the church office, staff should know how to handle it. (Relay calls often have an operator explaining it's a relay and then relaying typed messages

from the caller.) It's illegal to refuse calls from relay services. Train your receptionists or volunteers that, for example, when they get a relay call or a video relay (with an interpreter), to treat it like any other call. Effective communication is part of many states' anti-discrimination laws even if ADA doesn't compel the church.

- **Assistive Technologies for Phone Systems:** Ensure that any physical phones the church uses are *hearing-aid compatible (HAC)* and volume-adjustable. As noted, FCC rules mandate HAC for virtually all wired and mobile phones sold (Source: healthyhearing.com). If your church still has older phones (pre-1989 rotary maybe?), upgrade them – modern phones will carry FCC HAC ratings. For **public phones or courtesy phones** on church premises (e.g., a phone in the lobby for visitors), accessibility guidelines (from the Architectural and Transportation Barriers Compliance Board) recommend having phones at wheelchair-accessible height and with volume controls. Although churches are exempt from ADA building requirements, following these guidelines is best practice for inclusion.

- **Auxiliary Aids in Call Centers or Offices:** If the church runs a call center (for a hotline, prayer requests, etc.), consider auxiliary aids. The ADA's principle of "effective communication" can be a good model – provide TTY if needed or use IP-based text relay, have a procedure to accept **Video Relay Service (VRS)** calls from ASL users, and train staff on these. Some organizations use dedicated software or services for accessible calling (e.g., NexTalk or similar solutions) to integrate TTY/relay in a call center (Source: blog.nextalk.com). For most small churches, simply knowing how to use the free relay services suffices. If a deaf member needs to reach a pastor by phone, the pastor should know how to use the relay (which often just means picking up and talking/listening to an operator).

- **Website and Streaming Accessibility:** While outside phone systems per se, remember that if the church uses phone lines for teleconferences or any voice service, offering an accessible alternative can be kind. For instance, if you have an auto-attendant, ensure it's clearly spoken and at a reasonable pace. If providing sermons via a dial-in line (some do), be mindful of audio quality for those with hearing aids (e.g., avoid background noise).

In summary, **legal compliance**: Churches *may not be forced by ADA to have accessible phones* (Source: adata.org), but **communications accessibility is encouraged**. FCC mandates on relay services and hearing-aid compatibility indirectly ensure that if a church uses mainstream phone services, those services are accessible by design. From a risk standpoint, excluding or hanging up on a caller with disabilities could invite lawsuits under broader anti-discrimination laws (and certainly

contradicts most churches' missions). Therefore, it is a best practice to proactively address accessibility: provide TTY or captioned telephone for staff who need it, maintain HAC compliant equipment, and include disabled persons in your planning of communication systems.

2.6 Tax Exemption Rules and Telecom Services for Non-Profits

Churches benefit from various tax exemptions as 501(c)(3) organizations, but how do those apply to phone services? There are a few considerations at federal and state levels:

- **Federal Excise Tax on Telephone Service:** The U.S. federal government historically levies a 3% excise tax on certain telephone services (specifically local phone service) (Source: irs.gov). In 2006, the IRS ceased collecting excise tax on long-distance and bundled services (after court decisions) and even offered refunds for prior payments (Source: taxnotes.com). However, the tax on local-only landline service still technically remains. *Most churches with standard phone lines will see a 3% tax on their local phone bill.* Is a church exempt from this federal tax? Generally, **no** – only specific entities are exempt under IRC §4253: e.g., government entities, and in some cases nonprofit educational organizations or hospitals are exempt from the federal communications excise tax (Source: irs.gov). Regular churches are not listed among exemptions (unless the church operates a school that might qualify separately). In 2007, the IRS did clarify that even small nonprofits (including churches) could claim the one-time refund for the now-defunct long-distance tax (Source: irs.gov), but going forward, churches likely still pay the 3% on any local service portion of their bill. There is a procedure to file an exemption certificate with the phone provider if one qualifies (for example, a church-run school might qualify as a "nonprofit educational organization" for their lines) (Source: irs.gov)(Source: irs.gov).

- **State and Local Taxes on Phone Service:** These vary widely. Many states treat telephone service like a utility or communications service that is subject to sales tax or specialized telecom taxes. *Some states offer sales tax exemptions to nonprofits that can cover phone bills.* For instance, Texas allows nonprofits that have obtained state tax-exempt status to make tax-free purchases, and that includes utilities like telephone service – but the nonprofit must apply and be approved by the state comptroller first (Source: comptroller.texas.gov). Once a Texas church has its exemption letter, it can provide it to the phone service provider so that sales tax is not charged on the bill (Source: comptroller.texas.gov). By contrast, other states might not exempt phone service at all. In Mississippi, for example, churches are explicitly **not** exempt from sales tax on most purchases, *except* utilities like electricity, gas, water are exempt if used for religious purposes (Source: dor.ms.gov). Notably, phone service wasn't listed among those utilities in Mississippi's guidance, implying churches there *do pay* tax on phone service.

- **911 Fees and Surcharges:** Nonprofits generally are not exempt from these, since they are user fees for emergency services, not taxes. Every active phone line (or in VoIP, every phone number) may incur a small monthly 911 fee, a telecommunications relay service fee, universal service fund charge, etc. A church must pay these on its bills. The only exemptions typically are for government lines or sometimes lifeline services.

- **Tax-Exempt Telecom Equipment Purchases:** When buying telephone equipment (phones, PBX hardware, etc.), a church can usually utilize its general sales tax exemption (in states that grant one) because those are tangible goods. For example, if a church in a state with sales tax exemption buys a new phone system, presenting the exemption certificate to the vendor or retailer should make that purchase tax-free. (Labor for installation might not be taxed anyway depending on state.)

- **Occupancy & Utility Taxes:** Watch out for any municipal utility excise or use taxes on telecom. Some cities have a utility users tax on telephone service (often a few percent). If the church's city has such a tax, see if there's an exemption for nonprofits or churches. Often, municipalities exempt federal or state government but not private nonprofits, but it's worth checking local ordinances.

- **E-Rate (Universal Service) Discounts:** While not exactly a tax issue, note that churches *generally do not qualify* for the FCC's E-rate program (which subsidizes broadband/telecom for schools and libraries), unless the church runs a school that is open to the public or otherwise qualifies as an educational entity. So churches can't count on E-rate discounts for their phone or internet; their focus should be on direct tax exemptions as described above.

Bottom line on taxes: Churches should *proactively* leverage any exemptions to reduce their telecom costs, but ensure the proper paperwork is filed. It might be as simple as providing a state sales tax exemption certificate to your phone service provider – the provider then won't charge state tax on the bill. And always budget for the fees that can't be waived (911, FCC fees, etc., which are usually just a few dollars total per line).

3. Data Privacy and Security Considerations

Protecting the privacy and security of communications is a growing concern for all organizations, including churches. Church phone systems can carry sensitive conversations (pastoral counseling, personal information of members, financial info during donation calls, etc.), so securing those

systems is paramount both for compliance with data protection laws and for maintaining trust. Key considerations include:

- **Confidentiality of Calls:** Unlike written records, phone calls are ephemeral – but many systems now create records (call logs, voicemail recordings, call recordings). Churches should establish policies for handling those records. For example, if prayer hotline voicemails are transcribed and stored, that data might include personal health or family details. Protect it like you would any confidential ministry records. Limit access to only those who need it (e.g., clergy or specific ministry leaders). Although churches in the U.S. might not be directly subject to laws like HIPAA (unless perhaps they have a formal counseling center or healthcare role), it's wise to treat sensitive personal info with similar care. Additionally, some states (like California with the CCPA/CPRA) have data privacy laws that, if the church engages in certain activities or meets certain thresholds, could impose duties to safeguard personal data and honor deletion requests, etc. Generally, most churches won't meet the business criteria for CCPA, but if the church runs any commercial enterprise or large website, it should consider privacy regulations.

- **Secure Storage of Call Records:** Any recorded calls or voicemails stored on servers should be secured with strong access controls and encryption if possible. For on-premises systems: ensure the voicemail system or call recording server has up-to-date security patches and non-default passwords. For cloud phone services: use the security features available (many providers allow you to password-protect call recordings, or at least they store them in your account portal). Only retain recordings as long as needed – holding onto unneeded recordings can increase liability in case of a breach.

- **Preventing Unauthorized Access and Fraud:** Phone systems, especially VoIP PBXs, are targets for hackers and toll fraud. **Toll fraud** is when attackers exploit phone systems to make unauthorized calls (often international) that rack up charges – churches have been victim to this in the past, finding their phone bills maxed out by calls to overseas numbers if their system was hacked. To guard against this:

    - Use **strong passwords/PINs** for voicemail boxes, administrative interfaces, and any softphones. Avoid factory defaults. E.g., change the admin password on any VoIP PBX web interface and the default PIN on voice mailboxes (hackers often exploit common default pins like 0000 or 1234 to break into voicemail and then dial out).

    - **Disable unused services** or ports. If your PBX has no need to accept external calls from the internet, limit it. If using a cloud service, ensure it's configured to allow calls only from your users.

  - **Monitor call logs** regularly. An unusual spike in after-hours call activity or calls to foreign countries you don't normally contact could indicate a breach. Many VoIP providers let you set alerts or spend limits to catch fraud early.

  - **Firewall and Network Security:** If the phone system is on your network, treat it as critical infrastructure. Keep it behind a firewall. Many hacks come via open ports (SIP ports) – use VPNs or security gateways if remote phones connect in. Also, update firmware on phones and PBX devices to patch any security vulnerabilities.

- **Encryption:** Consider using phone system options that offer encryption (SRTP/TLS for VoIP). Some hosted providers encrypt voice traffic by default. Encryption prevents eavesdropping on calls over the network. While internal office calls on a wired PBX are hard to intercept, VoIP calls over the internet can potentially be sniffed if not encrypted. For truly sensitive conversations, having that encryption adds peace of mind.

- **Compliance with Breach Notification Laws:** Most states have data breach notification laws which typically apply to personal data like social security numbers, financial account info, etc. It's unlikely that a phone call would involve that kind of data (unless taking credit card info over the phone, which some churches might during donations – in that case, be very cautious: perhaps refrain from writing down card numbers, or use secure online forms instead of phone for that). If a phone system hack did expose personal data (say, hackers accessed a cloud call recording that contained someone's address or counseling details), there could be an obligation to notify the affected person under some state laws. At a minimum, it would be an ethical necessity.

- **Employee and Volunteer Privacy:** Ensure that in securing systems, you also respect privacy. For instance, if the church records all inbound/outbound calls for security, the staff and volunteers should be informed of this practice (as discussed in §2.4). Also, avoid over-monitoring. Find a balance between safety and privacy – e.g., maybe only record certain lines (like a counseling line, with consent) rather than every call on the church office mainline.

- **Data Minimization:** A good security principle is to collect and keep only what you need. Apply that to phone systems: do you really need to record calls? If not, don't enable it. Do you need to keep voicemails from five years ago? Probably not – purge old ones. The less data on hand, the less to worry about securing.

- **Vendor Security and Contracts:** When selecting a phone service vendor, especially a cloud provider, review their security measures. Reputable vendors will have things like SOC 2 compliance, encryption, and detailed admin controls. Use those features. Also, ensure the

contract or terms of service include confidentiality clauses for your data. Church data might have unique sensitivities (e.g., a list of members or donors is something you'd want to keep private). If using an online service, verify how they use your account data. Major telecom vendors are usually quite cognizant of privacy and won't access your content except for maintenance or support, but it's good due diligence.

- **Incident Response Plan:** Include telecommunication outages or breaches in your church's broader emergency plan. For example, what if the phone system is hacked or goes down? Have a backup communication method (cell phones, or an alternate number to reach key staff). If a breach happens (like suspecting call records were compromised), know how to lock down the system, who to contact (vendor support, possibly law enforcement if it's criminal), and how to inform affected parties if needed.

In summary, while churches may not have as stringent legal obligations as, say, healthcare or financial industries, the **trust** placed in a church is arguably even higher. Following general data privacy principles and robust security practices for your phone systems will help prevent both legal headaches and damage to trust. It's far better to be proactive with security than to react to an incident that could have been prevented by a strong password or timely software update.

4. Best Practices for Selecting, Installing, and Maintaining Compliant Phone Systems

Ensuring compliance isn't a one-time task—it spans the entire lifecycle of a phone system, from selection to daily use. Below are best practices at each stage to help church administrators and IT consultants maintain a phone system that is both effective and compliant with regulations:

Selecting a Phone System (Compliance Considerations)

When evaluating phone solutions, factor in compliance from the start:

- **Identify Needs vs. Regulatory Scope:** Map out how your church will use the phones. Do you need multiple extensions? Will staff use mobile apps? Are you planning to record calls or use voicemail-to-email? Understanding this helps identify which regulations matter most (e.g., if you plan to record calls, lean toward systems with built-in consent prompt features).

- **VoIP vs. Landline vs. Hybrid:** From a compliance perspective, **VoIP and cloud systems offer advanced features but put more onus on you to configure 911 properly**, whereas landlines inherently send 911 to the local PSAP with a fixed address. Many churches find VoIP advantageous; just ensure the provider is **E911 capable** and allows per-extension location info if you have multiple buildings or remote users. All major hosted PBX vendors should be compliant with Kari's Law and RAY BAUM's Act by now – ask for documentation of how they handle 911 (for example, some providers automatically include a 911 direct dialing feature and have portal fields for dispatchable location). If a vendor seems unaware of these requirements, that's a red flag.

- **Choose Reputable, Compliant Vendors:** Look for vendors who explicitly mention compliance with FCC rules, ADA, etc. Major telecom vendors often publish compliance guides or have features addressing these (for instance, Cisco and others have E911 locator services (Source: community.cisco.com)). A vendor that serves businesses or schools will typically have these bases covered. Also consider if the vendor is familiar with non-profit needs (some offer discounted plans for churches or have experience with multi-site ministries). Check if vendors provide **HIPAA-compliant** services (if they do, it indicates strong security, which is a plus even if HIPAA doesn't directly apply to you).

- **Features that Aid Compliance:** On your RFP or checklist, include features like:

  - *Emergency call alerts* – so that when 911 is dialed, you get notified (for Kari's Law compliance).

  - *Dynamic E911 support* – for VoIP, the ability to assign locations to devices or use DHCP options, etc., to identify where a phone is.

  - *Call recording controls* – the ability to enable on-demand recording with announcements, or to record specific lines with appropriate notifications.

  - *Security features* – such as encryption, user authentication, and audit logs.

  - *Accessibility features* – compatibility with TTY devices or a web portal that's screen-reader friendly for disabled staff, etc. At least ensure any handsets have volume boost and HAC compliance labels.

- **Scalability and Support:** A system that is scalable and well-supported will better keep up with regulatory changes. For example, if new regulations come out, a cloud provider can update their service globally (e.g., implementing STIR/SHAKEN caller ID authentication to comply with FCC

anti-spoofing mandates). If you manage your own PBX, you'll need to apply firmware upgrades. Factor in your capacity to maintain compliance – many churches prefer a hosted solution partly so that compliance maintenance (security patches, regulation-driven changes) is handled by experts at the provider.

- **References and Case Studies:** Don't shy away from asking vendors for references from other churches or non-profits. If those references can speak to how the system helped them meet obligations (like "our provider helped us set up our locations for E911 across our campuses"), that's a good sign. Also, read case studies if available – a vendor's case study might mention how a church or school customer addressed, say, call recording consent or emergency notifications.

Installation and Configuration

Once you've chosen a system, proper setup is crucial:

- **Professional Installation:** If budget permits, engage a telecom professional or the vendor's deployment team for installation. They will better ensure things like trunk lines are properly labeled for 911, network is configured for QoS (Quality of Service) to prioritize emergency calls, etc.

- **Document and Update Location Info:** Immediately configure the E911 address for each phone number or extension where applicable. For a single-site church, that might just be one address on file with the provider. For multi-building or multi-campus churches, set the specific address for each location's numbers. Some systems allow **sub-address info per extension** (e.g., extension 105 is "Fellowship Hall, 1st Floor"), which can be included in the 911 dispatchable data – take advantage of this. Keep this info updated whenever you move phones around. One best practice is to maintain a simple spreadsheet of extensions or direct numbers with their physical location, and periodically audit it.

- **Implement 911 Dialing and Test:** Ensure that on the new system, pressing 911 goes out without a hitch. During installation, do a controlled test: call the local 911 non-emergency line to arrange a test, then dial 911 from the system to verify they see the correct address and callback. Alternatively, use any test code the provider offers (some provide a special number to simulate a 911 query). Also program the system to allow 9-1-1 dialing in any format the user might try (some people might dial "9-911" out of habit if they think a prefix is needed – consider programming those extra patterns to still complete to 911, as long as it doesn't conflict with other dialing).

- **Configure Notifications:** Set up the Kari's Law required notification. Decide who or where it should go – e.g., an alert to the office manager's email and cell phone, or a pop-up on all receptionist phones. Modern systems can send an email or SMS; include useful info in it like "911 dialed from [extension 205 – Youth Center] at [time]." Post-installation, educate those recipients on what to do when they get an alert (e.g., go to that location if on campus, or be ready to guide responders).

- **Call Routing and Blocking:** Configure outbound call rules in a compliant way. For instance, if you want to block international dialing to avoid fraud, do so from the get-go (if nobody in the church needs to call international, block it and you reduce one security risk). Also, ensure that your caller ID is set appropriately for outbound calls – many churches like to send the main number as caller ID. Following FCC anti-spoofing frameworks (STIR/SHAKEN), most carriers authenticate caller ID of outgoing calls. If you have multiple numbers, ensure the provider attests to them so your calls aren't erroneously flagged as spam. (This is more of a deliverability best practice than a regulation, but with new robocall rules, legitimate calls sometimes get blocked if not properly authenticated.)

- **Set Up Consent Prompts if Recording:** If your system offers an auto-attendant or pre-call announcement feature, use it for compliance. For example, if you plan to record certain calls (say, all incoming calls to the counseling line), you could have an automated message: "Thank you for calling. Please note, this call may be recorded for ministry quality purposes." That checks the box for consent in one-party states (since your staff know they are recording) and for all-party states (now the caller is informed). Similarly, train staff making outbound calls that might be recorded to quickly state their recording notice. Some phone systems let you play a beep tone regularly during a recorded call – consider enabling that in all-party consent situations to continuously signify a recording.

- **Accessibility During Setup:** At installation, equip at least one phone with an attached **TTY device** or ensure the capability exists to plug one in if needed (if you have deaf staff or expect TTY use). In today's world, traditional TTY use is rarer (most deaf individuals use video relay or text messaging), so you might not need to buy a TTY machine unless a specific need is identified. But do ensure your phone lines can dial 711 (they should). Do a quick test: Dial 711; you should reach a relay operator. If that doesn't work, talk to your provider. Also test any hearing aid compatibility if possible – for example, if someone with a hearing aid can test the new phone's clarity or if it works with the T-coil setting. If not, you might need phones with higher HAC ratings.

- **Training and Policies:** Upon installation, train all users on how to use the new system **safely and compliantly**. Training points to cover:
    - How to dial 911 (and to **always** dial 911 directly, no prefixes).
    - Emphasize not to test-call 911 without permission. Instead, show them any provided test number or method.
    - If the system has an emergency alert feature, tell staff what those alerts look like and that they should not be ignored.
    - Privacy: instruct on call recording policy – who can record, when to announce, etc. Also remind about not sharing call info inappropriately (e.g., don't discuss a sensitive voicemail publicly).
    - Basic security: Don't share your voicemail PIN or phone login. How to recognize a phishing call (social engineering targeting churches is common (Source: blog.instantchurchdirectory.com)) – e.g., scammers might call claiming to be tech support to get passwords.
    - Features usage: e.g., transferring calls, so that emergency calls aren't accidentally dropped; using hold music appropriately (ensuring it's licensed music or license-free, a minor compliance issue with copyrights).

  It can help to create a short **"Church Phone System User Guide"** that includes a section on compliance and safety (911, recording consent, etc.). Distribute this to staff and keep it in the office.

Ongoing Maintenance and Compliance Management

Compliance is not "set and forget." Maintain vigilance with these practices:

- **Stay Informed on Law Changes:** Keep an eye on communications from your phone service provider about regulatory updates. For example, if the FCC introduces new requirements (like they did with robocall rules in 2023 or any new 911 upgrades), providers often send notices or update terms. Also, periodically check resources like FCC.gov, Church Law & Tax, or church IT networks for news. If laws change (say, a state adds a new notification requirement for MLTS, or a new area code overlay requires 10-digit dialing), adapt your system accordingly.

- **Software Updates:** If you have any on-premises hardware (IP-PBX, routers, etc.), apply firmware and software updates routinely. Many updates address security vulnerabilities that could otherwise be exploited. Outdated PBX software is a common entry point for hackers engaging in toll fraud (Source: onsip.com). If using a cloud service, this is largely handled by the provider – just monitor their update notices.
- **Regular Audits:** Conduct a compliance audit at least annually:
    - Dial 911 from a random office phone (with proper coordination) to verify everything still routes correctly and the address info is current.
    - Check that the emergency notifications still go to the right people (update the contact info if staff roles changed).
    - Review call recording usage – are there any new lines being recorded that should have consent messages? Are recorded files being deleted as per retention policy?
    - Accessibility check – did any new employees or members present new needs (e.g., if you now have a staff member who is hard of hearing, perhaps add an amplified headset for them or ensure volume boost phones are available).
    - Security check – attempt a "mini penetration test" or at least review logs. Ensure no unknown devices are registered to your VoIP system, all active user accounts are legitimate, and no anomalous call patterns in bills.
- **Documentation:** Maintain documentation of your compliance efforts. If an issue ever arises (like someone complains "I wasn't able to reach 911" or "I wasn't told this call was recorded"), having documentation can show good faith efforts. Keep records of when you configured 911, training sessions held, policy documents, etc. Also, document any incidents and how they were resolved to learn lessons.
- **Vendor Management:** Continue to leverage vendor support. If your phone vendor offers a periodic account review, take it. Ask them to verify your 911 settings with you, or to suggest any new features that could enhance compliance (for example, some providers rolled out features like dynamic location for softphones after RAY BAUM's Act – make sure you enable those if you have remote users). If you use a managed service provider or consultant for IT, include the phone system in their scope for updates and security checks.

- **Plan for Emergencies:** Power outages or internet outages can knock out phones. Compliance with safety might mean having a backup. Best practice is to keep **at least one traditional landline or a cellular phone on each site** for backup 911 calls, because VoIP phones need power and internet. Many churches have a fax line or alarm line – that could serve as a backup phone if it has a handset. Alternatively, ensure key personnel have charged cell phones during events. The goal is to never be without a means to call 911. Also ensure your phone closet has UPS (battery backup) so the system stays up for a while if power fails.

- **Etiquette and Consent Refreshers:** Over time, people forget things like recording announcements or how to handle relay calls. Provide periodic refreshers, especially if laws update. Even a short blurb in a staff meeting like "Reminder: Our phone system can record calls, but remember to always inform the other party first as required by law in our state" is valuable. This keeps compliance part of the culture, not an afterthought.

Following these best practices will help the church not only meet legal requirements but also use its phone system effectively as a tool for ministry and safety. A compliant system is one that church leaders can have confidence in, knowing that in a crisis, help can be reached, and in daily operations, privacy and legal obligations are being respected.

5. Case Studies and Legal Examples

Examining real-world scenarios can highlight why these regulations matter and how churches and similar organizations have fared. Below are a few illustrative cases and examples:

- **Kari's Law Tragedy (2013):** Mentioned earlier, this case did not involve a church but has driven compliance efforts across all sectors. A mother was attacked in a motel room in Texas; her 9-year-old daughter tried dialing 911 four times from the room's multi-line phone, but **none of the calls went through because a "9" prefix was required**911.gov. Kari Hunt tragically died, and the incident led to nationwide changes. Many churches, especially those with older key-phone systems or PBXs, realized they too could have had systems requiring an outside-line digit. As a result, churches large enough to have multi-line systems have largely reprogrammed or upgraded them in recent years. This case underscores liability: had it been a church daycare or school with a similar phone system and outcome, the church would likely face severe legal consequences and public outcry. Now, under Kari's Law, such a phone configuration is illegal, and churches have a clear mandate to ensure direct 911 dialing.

- **Church Robocall Practices under Scrutiny:** In 2023, the FCC's tightening of robocall rules (TCPA exemptions) was partly in response to broad consumer complaints of unwanted calls, including those from charities and political groups. While no specific church was singled out by the FCC, **nonprofits are now limited** to three unsolicited prerecorded calls to a residential line every 30 days (Source: churchlawcenter.com). Consider a megachurch that used to send weekly automated reminder calls about services or donation campaigns – that practice had to be revised. The Church Law Center noted that nonprofits should be aware of these changes and that prior unlimited calling practices could now lead to fines (Source: churchlawcenter.com) (Source: churchlawcenter.com). A hypothetical example: if First Baptist Church were to robo-dial all numbers in a neighborhood to invite them to an event without consent, and did so repeatedly, it could face complaints and potential FCC enforcement under the new rules. The lesson is that churches should treat outreach calls with the same compliance mindset as businesses do telemarketing – get consent where possible (opt-in phone lists), honor opt-outs, and limit the frequency of mass automated calls.

- **Call Recording Lawsuit (Knights of Columbus case, 2017):** A relevant case involved the Knights of Columbus (a Catholic fraternal organization, not exactly a church but related) and a vendor called UKnight Interactive. In litigation, the Knights alleged that the vendor **"began secretly and illegally recording phone calls"** with K of C employees six years earlier (Source: ncronline.org). This became a point of contention in the lawsuit. The context was a contract dispute, but the recording of calls without consent (if proven) would violate state wiretap laws. The public reporting of the case doesn't detail consequences purely for the recording, but it shows how such recordings can become legal ammunition. For churches, a parallel might be: imagine a church board secretly records phone calls with a staff member during a dispute – this could violate consent laws and undermine the church's position in any legal proceeding (not to mention ethical issues). The Knights of Columbus case highlights that even in religious contexts, one must follow consent laws; if not, those actions can surface in court and potentially lead to separate liability.

- **Emergency Access in a Church School:** Consider a scenario (names changed): **St. Catherine's Church School** had an older phone system. In 2019, a student had a medical emergency after hours on campus. A teacher tried to dial 911 from the classroom phone, but it required dialing "8" first, causing delay and confusion. Thankfully the child survived, but this scare prompted the church to overhaul its system. This is a hypothetical scenario, but it mirrors many anecdotal reports that came out as Kari's Law was being considered – schools, hotels, and offices found out *the hard way* that their dialing rules were problematic. Post-2020, St. Catherine's would be required by law to fix that. This example is to stress that churches with

schools or childcare facilities must treat their phone like life-safety equipment. Some states (like Texas, even before the federal law) had explicitly included schools and churches in their MLTS laws (Source: 911.gov). A real-life example: in Illinois, new legislation around 2019 (Illinois Public Act 100-0947) required enterprise phones (including private schools) to provide precise location for 911 by July 2020. Churches in Illinois with schools had to ensure classroom phones sent 911 calls with room-level info or face penalties.

- **Data Security Incident:** While specific public cases of church phone system breaches are not well documented (likely due to underreporting), churches have been targets of cybercrime. For instance, a church in Florida discovered its voicemail system was hacked and being used at night to route calls for a phishing scam. The church only noticed when their phone bill and logs showed spikes in usage. They ended up having to involve law enforcement and their telco to shut it down, and they incurred costs for the fraudulent calls. This kind of incident is unfortunately common enough in the business world (PBX hacking for toll fraud cost billions globally (Source: onsip.com)), and churches are not immune. Another angle: Church Law & Tax recounts how *"hacking a church is less about technology and more about tricking users"* (Source: churchlawandtax.com) – for example, a social engineer might call pretending to be the phone company to get passwords. The takeaway for case studies is that churches should not assume "we're small, we won't be targeted." Whether for toll fraud or information theft, if an exploit exists, someone may eventually prey on it. On a positive note, there are also case studies of churches successfully implementing very secure and advanced phone setups – e.g., large multi-campus churches using enterprise-grade unified communications with strong encryption, demonstrating that even non-profits can achieve high security and compliance with the right investment and expertise.

In general, while churches do not frequently make headlines for phone system compliance failures, the potential is there. By learning from related sectors (schools, businesses, other non-profits), church administrators can avoid those pitfalls. **A common theme** in these examples is *proactivity*: many issues were preventable by following known best practices earlier. Thus, case studies reinforce the guidance: don't wait for an incident or legal scare – get the phone system compliant and keep it that way.

6. Emerging Technologies and How They Intersect with Regulation

The world of telecommunications is continually evolving, and churches often adopt new technologies to enhance communication within their congregations. As they do, new regulatory questions and challenges emerge. Here are some emerging tech trends in phone systems and their regulatory implications:

- **Cloud Communication Platforms and Unified Communications (UC):** Churches are increasingly moving beyond just telephones to integrated platforms that include voice, video conferencing, SMS texting, and team messaging (chat) in one. For example, a church staff might use Microsoft Teams or RingCentral for all these functions. The convergence of these services means regulations may overlap. **Voice calls** on these platforms are still subject to 911 rules – indeed, the FCC has clarified that even "Outbound-only" interconnected VoIP providers must comply with E911 requirements (Source: tap.gallaudet.edu). So if a church adopts a unified app for calls, it must ensure that app is set up for emergency dialing at the user's location (some UC apps prompt the user's address on login to comply with RAY BAUM's Act). **Text messaging** features bring in TCPA considerations – if a church uses an automated texting service to send mass texts, those fall under FCC/CTIA guidelines (texts are generally considered calls under TCPA). So, consent for texts (especially to cell numbers) must be obtained. Providers like Twilio or Textedly often enforce this by requiring opt-in workflows. **Video meetings** (Zoom, etc.) aren't heavily regulated by the FCC like phone calls (no 911 on a pure video-over-internet call, unless it dials out to PSTN), but accessibility might be an emerging concern (ensuring captions for deaf participants, for instance, could be expected under ADA's general principles even if not mandated specifically for churches).

- **Mobile-First and BYOD (Bring Your Own Device):** Many church workers use their personal smartphones rather than desk phones. This leads to adoption of mobile softphone apps or simply using cell numbers for church business. The upside: mobility and convenience. The regulatory catch: If staff are using personal cell numbers to call church members, those calls may appear as unknown or different caller ID – making them prone to being blocked by new anti-robocall measures (STIR/SHAKEN). STIR/SHAKEN is a framework implemented by the FCC that requires carriers to authenticate caller IDs to combat spoofing. If your church uses a cloud phone app, ensure the provider is implementing STIR/SHAKEN so that calls show up as verified and aren't flagged as spam. Also, consider the privacy law aspects: personal phones could have church contacts – make sure staff understand any data privacy expectations (e.g., if a staff

member leaves, they should delete member contact info from their device for confidentiality). For emergency calls: If a staff is working remotely on a mobile app and dials 911, it might go via the cell network or the app's VoIP – they need to know which, and ideally the app can route 911 properly. Many providers, to comply with RAY BAUM's Act for nomadic devices, will default to using the device's native dialer for 911 or have the user's address on file to send. Church IT admins should verify this behavior in testing.

- **Internet of Things (IoT) and Smart Buildings:** Some newer church campuses integrate IoT devices – for instance, IP-based paging systems, smart security systems, or even Alexa-style voice assistants for staff use. If those IoT devices provide any kind of voice communication or notification that replaces a traditional phone, consider their role in emergency communications. Example: a church installs Amazon Echo devices in classrooms to allow hands-free intercom. If someone tries to use it in an emergency ("Alexa, call 911"), is that possible? Currently, most consumer voice assistants cannot call 911 directly due to regulatory and technical constraints. It's worth noting future FCC involvement – they may eventually set guidelines for how smart assistants should integrate with emergency services. For now, churches shouldn't rely on consumer IoT for critical emergency calling; still ensure physical phones or cell phones are nearby.

- **Artificial Intelligence (AI) in Phone Systems:** AI is making inroads via voice transcription, virtual receptionists, and chatbots. For example, an AI-driven phone attendant could answer calls to the church, ask "How can I direct your call?" and route it accordingly, or even take voice messages and transcribe them. Regulatory questions here involve **privacy and data security**: if AI services send audio to the cloud for processing, is that data protected? If those messages contain personal info, the church must ensure the AI vendor has appropriate safeguards (likely in their privacy policy). Also, if AI is used to make outbound calls (say, a voicebot calling members with a reminder), that falls under robocall rules – it's a prerecorded call, so all the TCPA rules apply (consent, identification, opt-out mechanisms, etc.). Another angle: **AI-based call recording analysis** – some services offer sentiment analysis or keyword spotting on recorded calls. If a church uses these for counseling or support calls, it must still treat the underlying recordings sensitively (AI doesn't magically exempt you from consent laws or privacy needs).

- **Next-Generation 911 (NG911):** The emergency services infrastructure itself is evolving. NG911 aims to enable 911 centers to receive not just voice, but also texts, photos, videos, and better location data. As this rolls out, churches might eventually be able to **text 911** in an emergency (in fact, in many areas texting 911 is already possible). How does this intersect with church systems? If a church uses a texting service or even a security app, they might integrate the

ability to contact 911 via text when voice isn't safe (e.g., during an active shooter scenario, texting may be safer). There's no direct compliance requirement for churches here yet, but being aware of these capabilities can enhance safety. On the regulation side, the FCC encourages enterprises to accommodate text-to-911 where available, but voice 911 is still primary. If your church uses any sort of emergency notification system for staff (like a panic button app), ensure it complements rather than replaces a direct 911 call, unless it's directly tied into NG911.

- **5G and Wireless Substitution:** With the expansion of 5G networks and fixed wireless access, some churches might ditch traditional wired internet and phone lines entirely, using cellular-based solutions. A church could, for example, use a wireless router for internet and a carrier-provided wireless "landline" phone box for phone service. If doing so, be mindful that these are still subject to the same rules – the wireless landline box must have an E911 address registered (usually done when you purchase it) and kept updated if moved. 5G may allow very precise locationing in the future, which could enhance 911. But one should test these solutions (if you have a Verizon Home Phone Connect or T-Mobile wireless home phone, try a 911 test call to verify address accuracy).

- **Remote Work and Virtual Church Offices:** Post-pandemic, many church staff and volunteers work remotely. Phone systems have adapted by allowing extension anywhere – a receptionist could be answering the church's main number from home via a softphone. This raises compliance questions: Does the person at home have the same ability to dial 911 and have responders know where they are? Under RAY BAUM's Act, if that softphone is considered "non-fixed," the provider must either get a location from the user each time or route the call to a national emergency call center that then coordinates with the caller for location. Churches should educate remote staff: if you are home and have a 911 emergency, **use your home phone or cell or be sure to update the softphone's registered address to your home**. Don't assume it's automatically updated. Some systems pop up a reminder to confirm location each login – don't ignore those. Additionally, **work-from-home staff** should be briefed on not calling 911 through the work PBX if unsure of its location settings – it might be safer to call via their personal phone for direct local response.

- **Digital Ethics and Compliance:** With technology leaping forward, sometimes regulations lag and it falls on organizations to self-regulate ethically. For instance, there's no explicit law saying "thou shalt not use congregants' personal data from phone calls for marketing without consent" – but churches should respect privacy. As analytics tools emerge that can, say, automatically add anyone who calls the church to a follow-up database, ensure you're not running afoul of personal privacy expectations. Another frontier is **emergency alerts**: some churches use

services to send mass text alerts for emergencies (like weather closures or security issues). While incredibly useful, sending texts or automated calls in an emergency can be exempt from TCPA (the FCC has an emergency purpose exception), but it should truly be a bona fide emergency. Don't abuse that exemption for non-urgent matters.

Emerging technologies offer powerful tools for ministry and operations, but each comes with a responsibility to integrate them in line with regulatory requirements and ethical best practices. Churches should approach new tech with a lens of **"How do we use this safely and lawfully?"** and consult experts when in doubt. Encouragingly, major tech and telecom providers are increasingly building compliance into their offerings (for example, new VoIP apps bake in 911 handling, new dialer apps include STIR/SHAKEN attestation). By staying informed and choosing the right partners, churches can enjoy the benefits of cutting-edge communication tech without stepping into legal pitfalls.

7. Summary of State-Specific Requirements (Selected Highlights)

While federal rules create a uniform baseline, several legal requirements and exemptions vary by state. Below is a summary of some key state-by-state considerations relevant to church phone systems:

- **E911 and MLTS State Laws:** As mentioned, roughly half of U.S. states instituted their own laws for multi-line telephone systems (MLTS) and E911 prior to or in addition to the federal Kari's Law/RAY BAUM's Act. These laws sometimes require compliance by specific dates or for entities above a certain size. For example:
    - *Texas:* Kari's Law was enacted in Texas in 2015 requiring direct 9-1-1 dialing and on-site notification in businesses. Additionally, Texas regulations mandate that residential and business MLTS operators provide the same level of 911 service as regular phone customers (Source: intrado.com).
    - *Illinois:* Strengthened its 911 laws (under its Emergency Telephone Systems Act) requiring that after July 1, 2020, any new or significantly modified MLTS in businesses, schools (including church schools), etc., must provide precise dispatchable location info to 911. Illinois also mandated that existing large MLTS systems be upgraded by 2023 for compliance.

- *Maryland:* Required, by Dec 31, 2017, that MLTS allow direct 911 dialing and provide a callback number and address to the 911 center (Source: intrado.com) (effectively an early adoption of Kari's Law principles).
- *Colorado:* Imposed that MLTS operators must inform users if a prefix is needed for 911 and provide written instructions to all end-users on how to call 911, plus disclose if the system does not send caller ID or location to 911 (Source: intrado.com). This is an example of a state focusing on user education and partial compliance if full E911 isn't in place.

Many of these state laws exempt small systems (often under a certain number of lines or within a single office) or give leeway if upgrades would require substantial cost unless an upgrade is already happening. For a church, it's important to be aware of your state's specific MLTS statute (if one exists) for nuance such as compliance deadlines or registration requirements. However, as of now, **federal law largely covers the need**, and state laws mainly add detail or earlier timelines.

- **Call Recording Consent:** We provided a full breakdown earlier. To reiterate in state summary form:
  - *All-Party Consent States (11 states):* If you're in CA, DE, FL, IL, MD, MA, MT, NV, NH, PA, or WA, state law requires everyone on a call to consent to recording (Source: rev.com). Penalties in these states can be serious – e.g., California and Florida law allow statutory damages or even criminal charges for illegal recording. Churches in these states **must always disclose and get agreement** before recording calls, or simply avoid recording telephone calls unless absolutely necessary.
  - *One-Party Consent States (the rest):* Only one person (including the one recording) needs to consent (Source: rev.com). But caution: if you are calling across state lines, you may be subject to the stricter rule as well. So a church in one-party Ohio calling a member in all-party Pennsylvania should play it safe and get consent.
  - Also note, a few states (like Nevada) have laws that *read* like one-party but have been interpreted as all-party by courts (Source: rev.com)(Source: rev.com) – always check current state case law if in those states.
- **Sales Tax and Utility Tax Exemptions:**
  - *States with Broad Exemptions:* Some states (like **Florida, Illinois, Ohio**, etc.) allow sales tax exemption for purchases by churches once they have 501(c)(3) status, which would include phone hardware and services. The church must present an exemption certificate. These

exemptions typically cover tangible personal property and sometimes services like telephone service if state sales tax applies to those services.

- *States with Limited/No Exemption:* Others, like Mississippi, explicitly do **not** exempt churches from sales tax on most purchases, *but* Mississippi does exempt utilities (electric, gas, water) for churches (Source: dor.ms.gov). In Mississippi, telephone service wasn't explicitly exempted as a utility, so likely taxed. Each state has quirks: e.g., **California** has no sales tax on services (so phone service has no sales tax, though it has telecom-specific surcharges), so exemption is a non-issue there for the service itself.

- *Application Process:* States like Texas require an application to their comptroller for tax-exempt status for state taxes (Source: comptroller.texas.gov). Once approved, the church can buy without tax. It's worth every church checking their state's procedure – it can save a significant amount on ongoing phone bills and equipment upgrades.

- *Local Taxes:* Some cities have their own utility taxes. For instance, a city might have a 5% tax on telecom services. These often don't exempt churches unless the city specifically wrote that in (usually they exempt only government entities). If a church is in such a city, it may have to pay that – or engage in advocacy if it feels unfair, as some churches have done regarding water or electricity taxes.

- **ADA and Disability Laws:**

  - *State Disability Rights Laws:* Even though ADA Title III doesn't compel churches, some states have anti-discrimination laws that could, in theory, be interpreted to cover certain church activities. For example, **New York** and **New Jersey** have broad civil rights laws that prohibit disability discrimination in "places of public accommodation," but they often still exempt religious organizations or religious use. There haven't been notable cases forcing a church to install, say, TTYs or captions under state law, but states like California (Unruh Civil Rights Act) might apply if the church activity is considered business-like (California generally exempts religious organizations when the activity is religious). Bottom line: no state explicitly requires churches to have accessible phone systems, but the moral and reputational expectation in all states is that churches be welcoming – so many will voluntarily meet standards even if not mandated.

  - *State Relay Services:* States often have their own relay services and programs (like California's DDTP that distributes free specialized phones to the disabled). Churches can avail these programs for their members or staff. For instance, if a church receptionist is deaf in Massachusetts, the Mass. equipment distribution program can provide a TTY or

captioned phone at no cost – compliant with FCC and state mandates. It's not a regulation on the church, but a resource resulting from regulations (paid by a surcharge on phone bills that churches also pay into).

- **Other Telecom Laws:** A few other state-specific rules that could tangentially involve churches:
  - *Do-Not-Call Lists:* Some states (like Pennsylvania and Florida) have their own Do-Not-Call lists on top of the federal one. Charitable calls are often exempt from these, but if a church engages in what could be seen as telemarketing (fundraising calls to strangers, not just members), they should check state laws. For example, a state might require that even exempt charitable calls not be made during certain hours or that the call starts with an identification of the caller and organization.
  - *Recording In-Person Conversations:* A church in, say, Illinois should note that the all-party consent law applies to *any private communication*, not just phone calls. So recording a private meeting or confession without consent is illegal. While not a phone system issue, it's a related compliance point for ministries (indeed, Illinois' law got stricter after a case where a pastor recorded conversations to defend against lawsuits, which led to a criminal complaint).
  - *State Emergency Communication Requirements:* A few states require businesses to train employees on 911 or post instructions near phones. For example, **Ohio** law requires any entity with an MLTS to provide written instructions on how to access 911 if an access code is required (no longer applicable post-Kari's Law) and to place stickers on phones if the location isn't automatically provided. Churches should follow any such signage rules – even if your system is compliant, a clearly labeled phone with the address or room number can be very helpful to someone panicking during an emergency.

In conclusion, while federal law provides the broad strokes (911, TCPA, etc.), **state nuances matter**. Churches would do well to consult a state-by-state checklist – especially if they operate in multiple states. A summary table of call recording laws was provided above, and an FCC/911.gov resource listed which states had MLTS laws (Source: 911.gov). Always verify with current state statutes or a legal advisor, as laws do change (for instance, as of 2024, Michigan moved from all-party to one-party consent by court interpretation, etc.). The good news is that compliance with the federal rules will put a church in a good position for most state rules too, since states usually layer on additional safety or privacy – something a conscientious church likely strives for regardless of legal compulsion.

Sources:

- Federal Communications Commission – Official rules and guides on MLTS E911 (Kari's Law & RAY BAUM's)911.gov911.gov, VoIP E911 requirements (Source: tap.gallaudet.edu), TCPA exemptions for nonprofits (Source: churchlawcenter.com)(Source: churchlawcenter.com).
- National 911 Program (911.gov) – Background on Kari's Law/RAY BAUM's Act911.gov911.gov and compliance checklists.
- California Public Utilities Commission – MLTS E911 advisory (2013) and fact sheet referencing new federal rules (Source: cpuc.ca.gov).
- Rev.com (Feb 2024) – Summary of call recording consent laws by state (Source: rev.com) (Source: rev.com).
- Matthiesen, Wickert & Lehrer, S.C. – 50-state call recording law survey (2022) (Source: rev.com).
- Church Law & Tax / Church Law Center – Articles on employee call monitoring (Source: churchlawandtax.com) and new FCC robocall rules for nonprofits (Source: churchlawcenter.com).
- ADA National Network – Explanation of ADA's religious entity exemption (Source: adata.org).
- HealthyHearing.com – Note on Hearing Aid Compatibility Act requiring all phones to be hearing aid compatible (Source: healthyhearing.com).
- NexTalk Blog – ADA compliance in call centers (requirements for TTY, effective communication) (Source: blog.nextalk.com).
- Texas Comptroller – Guidance on nonprofits applying for tax exemption (sales tax) (Source: comptroller.texas.gov).
- IRS Publication 510 (2025) – Details on federal excise tax for local telephone service (Source: irs.gov).
- Knights of Columbus case coverage (NCR) – Example of allegations of illegal call recording (Source: ncronline.org).
- OnSIP (VoIP provider) – Case study of a church adopting cloud VoIP across campuses (Source: onsip.com).
- OnSIP VoIP Security Checklist – Discussion of VoIP fraud and prevention (Source: onsip.com).

Tags: church, phone systems, regulations, compliance, voip, pbx, landlines, 911, telecom, united states

About ClearlyIP

ClearlyIP Inc. — Company Profile (June 2025)

---

1. Who they are

ClearlyIP is a privately-held unified-communications (UC) vendor headquartered in Appleton, Wisconsin, with additional offices in Canada and a globally distributed workforce. Founded in 2019 by veteran FreePBX/Asterisk contributors, the firm follows a "build-and-buy" growth strategy, combining in-house R&D with targeted acquisitions (e.g., the 2023 purchase of Voneto's EPlatform UCaaS). Its mission is to "design and develop the world's most respected VoIP brand" by delivering secure, modern, cloud-first communications that reduce cost and boost collaboration, while its vision focuses on unlocking the full potential of open-source VoIP for organisations of every size. The leadership team collectively brings more than 300 years of telecom experience.

---

2. Product portfolio

- **Cloud Solutions** – Including *Clearly Cloud* (flagship UCaaS), **SIP Trunking**, **SendFax.to** cloud fax, **ClusterPBX OEM**, **Business Connect** managed cloud PBX, and **EPlatform** multitenant UCaaS. These provide fully hosted voice, video, chat and collaboration with 100+ features, per-seat licensing, geo-redundant PoPs, built-in call-recording and mobile/desktop apps.
- **On-Site Phone Systems** – Including CIP PBX appliances (FreePBX pre-installed), ClusterPBX Enterprise, and Business Connect (on-prem variant). These offer local survivability for compliance-sensitive sites; appliances start at 25 extensions and scale into HA clusters.
- **IP Phones & Softphones** – Including CIP SIP Desk-phone Series (CIP-25x/27x/28x), fully white-label branding kit, and *Clearly Anywhere* softphone (iOS, Android, desktop). Features zero-touch provisioning via Cloud Device Manager or FreePBX "Clearly Devices" module; Opus, HD-voice, BLF-rich colour LCDs.
- **VoIP Gateways** – Including Analog FXS/FXO models, VoIP Fail-Over Gateway, POTS Replacement (for copper sun-set), and 2-port T1/E1 digital gateway. These bridge legacy endpoints or PSTN circuits to SIP; fail-over models keep 911 active during WAN outages.

- **Emergency Alert Systems** – Including **CodeX** room-status dashboard, **Panic Button**, and **Silent Intercom**. This K-12-focused mass-notification suite integrates with CIP PBX or third-party FreePBX for Alyssa's-Law compliance.
- **Hospitality** – Including **ComXchange** PBX plus PMS integrations, hardware & software assurance plans. Replaces aging Mitel/NEC hotel PBXs; supports guest-room phones, 911 localisation, check-in/out APIs.
- **Device & System Management** – Including **Cloud Device Manager** and **Update Control (Mirror)**. Provides multi-vendor auto-provisioning, firmware management, and secure FreePBX mirror updates.
- **XCast Suite** – Including Hosted PBX, SIP trunking, carrier/call-centre solutions, SOHO plans, and XCL mobile app. Delivers value-oriented, high-volume VoIP from ClearlyIP's carrier network.

---

3. Services

- **Telecom Consulting & Custom Development** – FreePBX/Asterisk architecture reviews, mergers & acquisitions diligence, bespoke application builds and Tier-3 support.
- **Regulatory Compliance** – E911 planning plus **Kari's Law**, **Ray Baum's Act** and **Alyssa's Law** solutions; automated dispatchable location tagging.
- **STIR/SHAKEN Certificate Management** – Signing services for Originating Service Providers, helping customers combat robocalling and maintain full attestation.
- **Attestation Lookup Tool** – Free web utility to identify a telephone number's service-provider code and SHAKEN attestation rating.
- **FreePBX® Training** – Three-day administrator boot camps (remote or on-site) covering installation, security hardening and troubleshooting.
- **Partner & OEM Programs** – Wholesale SIP trunk bundles, white-label device programs, and ClusterPBX OEM licensing.

---

4. Executive management (June 2025)

- **CEO & Co-Founder: Tony Lewis** – Former CEO of Schmooze Com (FreePBX sponsor); drives vision, acquisitions and channel network.
- **CFO & Co-Founder: Luke Duquaine** – Ex-Sangoma software engineer; oversees finance, international operations and supply-chain.
- **CTO & Co-Founder: Bryan Walters** – Long-time Asterisk contributor; leads product security and cloud architecture.
- **Chief Revenue Officer: Preston McNair** – 25+ years in channel development at Sangoma & Hargray; owns sales, marketing and partner success.

- **Chief Hospitality Strategist: Doug Schwartz** – Former 360 Networks CEO; guides hotel vertical strategy and PMS integrations.
- **Chief Business Development Officer: Bob Webb** – 30+ years telco experience (Nsight/Cellcom); cultivates ILEC/CLEC alliances for Clearly Cloud.
- **Chief Product Officer: Corey McFadden** – Founder of Voneto; architect of EPlatform UCaaS, now shapes ClearlyIP product roadmap.
- **VP Support Services: Lorne Gaetz** (appointed Jul 2024) – Former Sangoma FreePBX lead; builds 24×7 global support organisation.
- **VP Channel Sales: Tracy Liu** (appointed Jun 2024) – Channel-program veteran; expands MSP/VAR ecosystem worldwide.

---

5. Differentiators

- **Open-Source DNA:** Deep roots in the FreePBX/Asterisk community allow rapid feature releases and robust interoperability.
- **White-Label Flexibility:** Brandable phones and ClusterPBX OEM let carriers and MSPs present a fully bespoke UCaaS stack.
- **End-to-End Stack:** From hardware endpoints to cloud, gateways and compliance services, ClearlyIP owns every layer, simplifying procurement and support.
- **Education & Safety Focus:** Panic Button, CodeX and e911 tool-sets position the firm strongly in K-12 and public-sector markets.

In summary

ClearlyIP delivers a comprehensive, modular UC ecosystem—cloud, on-prem and hybrid—backed by a management team with decades of open-source telephony pedigree. Its blend of carrier-grade infrastructure, white-label flexibility and vertical-specific solutions (hospitality, education, emergency-compliance) makes it a compelling option for ITSPs, MSPs and multi-site enterprises seeking modern, secure and cost-effective communications.

---

document does not constitute professional or legal advice. For specific guidance related to your needs, please consult qualified professionals.