PiPcall

eBOOK

Modern Mobile Communications Compliance in UK Rail

Navigating New Regulatory Standards for Call Recording

PiPcall delivers call recording over the Mobile Voice Network, secure cloud storage, and instant deployment across your rail workforce — no new phones required, and all managed from one central platform.

www.pipcall.com/so/rail-industry-mobile-compliance

Contents

Chapter 1: The New Rules of Rail Communication

Rail's Safety Backbone is Built on Spoken Words

In the UK rail industry, safety isn't just a matter of procedures and signals—it's built on precise, high-stakes conversations. The clarity, accuracy, and traceability of those spoken communications now carry more weight than ever.

Every verbal instruction between signaller and driver, every call made by a Controller of Site Safety (COSS), every emergency alert from a Mobile Operations Manager (MOM) — they are all classed as Safety Critical Communications (SCCs). According to Network Rail, failure to monitor, record, or manage these interactions correctly can be a direct contributor to incidents and near misses.

As a result, SCCs are now governed by a growing framework of regulatory guidance that applies not just to Network Rail personnel, but to the entire rail ecosystem — from principal contractors to subcontracted engineering firms, umbrella contractors, and beyond.

Why the Focus on Recording Now?

Several regulatory drivers have aligned to make call recording not just best practice — but an operational necessity:

- New modules from Network Rail's NR/L3/OPS/301 framework (effective March 2026) require voice recording across a wide range of roles and scenarios.
- Communication Review Groups (CRGs) must regularly assess recorded calls to track performance and implement corrective actions.

- Post-incident investigations demand fast access to call data — with detailed retention protocols and security standards.
- Mobile roles such as PICOPs, COSS, MOMs, and Engineering Supervisors increasingly operate across mixed device environments — often outside traditional GSM-R or OCS coverage zones.

And with the industry moving more operations in-house, contractors and service providers are facing tighter oversight, stricter audits, and more formal compliance reviews.

The Compliance Stakes Just Got Higher

Historically, many rail firms used legacy systems (signal box concentrators, radios, or GSM-R) to meet comms requirements. But these tools weren't designed for:

- Modern mobile-first teams
- Subcontractors on personal devices
- BYOD scenarios or umbrella workers
- Instant retention and investigation support

As one trackside contractor recently put it:

"ISS sponsors my tickets, but I'm technically under an umbrella company. They've got to prove I'm compliant — but I use my own phone. So, who's recording my calls?"

This question now matters. Because under the new Network Rail guidance, if you're not recording those calls, you're not compliant.

Chapter 2: What NR/L3/OPS/301 Means for You

Breaking down the key regulations that now shape rail communication compliance

A Shift from Policy to Practice

Network Rail's NR/L3/OPS/301 framework is no longer just guidance — it's a structured operating standard with measurable requirements for how rail teams communicate, monitor, and investigate.

For anyone managing operations, safety, or compliance — whether you're inside Network Rail or part of its extensive contractor base — this framework introduces a major operational shift. It moves rail communications from informal procedure into a disciplined, trackable, auditable system.

So, what does it actually require?

At a Glance: The Key Modules That Matter

Here are the modules and their practical implications for mobile communications:

1. NR/L3/OPS/301/01 – Recording Systems and Access

"Every signalling location, Route Control and Electrical Control Room (ECR) shall have voice recording capabilities, including contractors."

- Verbal communications must be recorded for critical safety tasks.
- Applies to Network Rail and all third-party workers engaged in safety-critical roles (COSS, PICOP, MOM, ES, etc.).
- Mobile users not connected to GSM-R or in areas without signal box concentrators must be covered by alternative compliant recording methods.

2. NR/L3/OPS/301/04 – Communication Review Groups (CRGs)

"CRGs shall jointly monitor the effectiveness of SCCs, agree targets, and report progress."

- Local and regional CRGs must assess and rate recorded calls every 12 weeks.
- Monitoring extends to subcontractors and support roles — including those using personal mobile phones on site.
- All CRG meetings held via Teams must be recorded and stored in line with GDPR and Network Rail's Corporate Records Retention Schedule.

3. NR/L3/OPS/301/05 – Incident and Operational Investigations

"Voice recordings must be available for review post-incident and retained securely by authorised persons."

- Recordings must be accessible for incident response and legal investigations.
- Only authorised personnel can download or handle media — with clear processes for retention and chain of custody.
- Non-compliance (e.g., failure to record, improper access, missing files) creates operational and legal risk.

The Operational Challenge

Many teams in rail infrastructure work with:

- Mixed-device fleets (BYOD + company phones)
- Contractors sponsored by umbrella orgs
- Limited access to GSM-R or NICE/Uniphore platforms
- Patchy signal areas (rural tracks, tunnels, remote junctions)

This results in gaps in call recording, particularly for mobile users — which now puts companies at odds with Network Rail's formal requirements.

PiPcall Insight

Where these standards say "must have recording capability," what's really needed is:

- A mobile solution that routes calls over the Mobile Voice Network and records automatically at the network level — with no recordings stored on the device or in an app
- One that can be rolled out to contractors, subcontractors, or umbrella workers, including those using personal phones
- Centrally managed through a secure portal, with full audit trails and admin-controlled permissions
- Secure, cloud-based storage with fast access for investigations, safety reviews, or CRG compliance

Chapter 3: Beyond GSM-R – Fixing the Compliance Gap

The Hidden Weak Link in Rail Communications

Most rail professionals are familiar with GSM-R (Global System for Mobile Communications – Railway), the dedicated communication platform for train control and signalling. It's reliable, it's standardised, and it forms the backbone of fixed and on-train comms.

But here's the problem: GSM-R doesn't cover everyone.

Contractors, maintenance engineers, COSS, MOMs, supervisors, and countless third-party staff working in the field — they're often outside the scope of GSM-R systems. These workers rely on personal or company-issued mobile phones, many operating on consumer-grade platforms with:

- No automated call recording
- No centralised storage
- No way to prove compliance during an audit or incident investigation

This is where most rail teams unknowingly face a compliance blind spot.

What the Regulations Assume — But Real Life Undermines

According to NR/L3/OPS/301/01, any individual involved in safety-critical communications must have their calls recorded. This includes situations where:

- Control rooms call a contractor onsite for task updates
- MOMs instruct on fault responses via mobile
- COSS calls a PICOP or signaller from a personal phone
- Supervisors escalate issues in real-time from remote sites

In theory, this means every device used for operational communications should support compliant, tamper-proof, retrievable call recording.

In practice? Most mobile phones in the field — especially BYOD (bring your own device) setups — fall well short.

Why Consumer Mobile Isn't Enough

The typical work-issued or personal mobile phone is not designed for regulatory-grade oversight:

Feature	Consumer Mobile	Regulatory Requirement
Call recording	Native call recording or VoiP apps	Automatic, enforced
Data storage	Local, vulnerable	Secure, cloud-based
Access controls	None or basic	Admin-controlled portal
Retention policy	User discretion	90+ day compliance standard
Incident support	Manual at best	Timestamped, exportable, auditable

Even where third-party call recording apps are used, they often rely on VoIP, which is susceptible to unreliable quality and can cause the mobile battery to drain faster.

The Risk Multiplier: Contractors & Umbrella Workers

In field interviews, engineers and rail contractors frequently described a web of device inconsistency:

"Everyone's got a different setup. One guy's on his own phone, someone else is on a company iPhone. The sponsor might record calls, but nobody really knows if the subcontractor's calls are being saved."

This lack of standardisation not only puts organisations at risk during compliance reviews — it also weakens their response readiness during incidents, near misses, or formal investigations.

What a Fix Looks Like

To close the compliance gap, rail teams need a mobile communication solution that:

- Is a network agnostic solution working on any UK mobile network
- Records calls over the Mobile Voice Network — not VoIP
- Stores recordings securely in the cloud and not on the device — accessible for authorised personnel
- Covers any mobile device — company-issued, personal, or umbrella-supplied
- Provides admin oversight — with call logs, search filters and access restrictions
- Scales easily — from 10 to 10,000 users across varied field structures

In short, a solution like PiPcall.

Chapter 4: Monitoring, Evidence, and Real-World Investigations

When the Call Log Becomes a Case File

In the rail industry, incidents don't just trigger repairs — they trigger investigations. And those investigations increasingly hinge on one crucial form of evidence: recorded verbal communication.

From near-misses and SPADs (Signals Passed At Danger) to line block infringements or emergency callouts, the ability to retrieve, audit, and verify mobile communications is now a cornerstone of compliance under Network Rail's operational rules.

The updated NR/L3/OPS/301 framework makes this crystal clear: your teams must be able to produce recordings on demand — securely, promptly, and with audit-ready accuracy.

What the Regulations Say

The requirements around post-incident communication are laid out most explicitly in NR/L3/OPS/301/05:

- All voice recordings must be retained if they relate to a safety incident
- Only authorised personnel (usually the Lead Investigator) may access or export them
- Retained audio must be isolated from those involved and stored in accordance with Network Rail's investigation protocols
- Any editing, deletion, or unauthorised access is a compliance breach

"Voice recordings may be used as evidence in an investigation and must be retained accordingly."
— NR/L3/OPS/301/05 Clause 6.1

This doesn't just apply to fixed equipment like GSM-R consoles or concentrators. It applies to any mobile phone used in the course of duty.

What Happens in the First 24 Hours

Here's a simplified breakdown of how verbal communication is used after an incident:
1. Initial response: Control teams or MOMs initiate containment and escalation by phone.
2. Investigation begins: Lead investigator seeks access to relevant call recordings.
3. Call logs reviewed: Timestamps, participants, and call content are extracted.
4. SCC reviewed: Was the safety-critical comms protocol followed?
5. Report generated: Communication failures or successes are documented in the outcome.

This means any unrecorded mobile call is not just a missed opportunity — it's a compliance gap that could:

- Delay the investigation
- Undermine safety learnings
- Lead to legal or reputational risk

The Cost of Missing Audio

Imagine a near miss involving a track possession team led by a COSS using a personal mobile. The signaller made a late change. The COSS insists the change wasn't communicated clearly.

If that call isn't recorded:

- There's no audio evidence
- No way to verify protocol adherence
- No ability to defend or hold accountable

"Worst thing is when you've got half the story on tape and the rest on someone's iPhone with no idea if it's recorded."
— Supervisor, Rail Maintenance Contractor

Chapter 5: How PiPcall Delivers Rail-Ready Compliance

Built for How Rail Really Works

Rail infrastructure isn't just complex — it's operationally fragmented.

Your workforce might include:
• Full-time Network Rail employees
• Subcontracted field engineers
• Sponsored contractors
• Mobile staff working remotely from depots, cabins, or trackside

Each person might use a different mobile setup — and yet, every safety-critical call they make or receive needs to be recorded, stored, and retrievable.

PiPcall is designed specifically for these real-world conditions.

Automatic Call Recording — No User Action

Calls initiated via the PiPcall app are routed over the mobile voice network — not VoIP — ensuring resilient, compliant-quality recording. Recordings are stored securely in the PiPcall Portal and not dependent on the user or the device.

That means:
• Calls are crystal clear, even in low-bandwidth areas
• There's zero reliance on Wi-Fi
• No one has to hit "record" — it just works

This aligns directly with Network Rail's expectations in NR/L3/OPS/301/01 and /05, which mandate passive, reliable recording for operational calls.
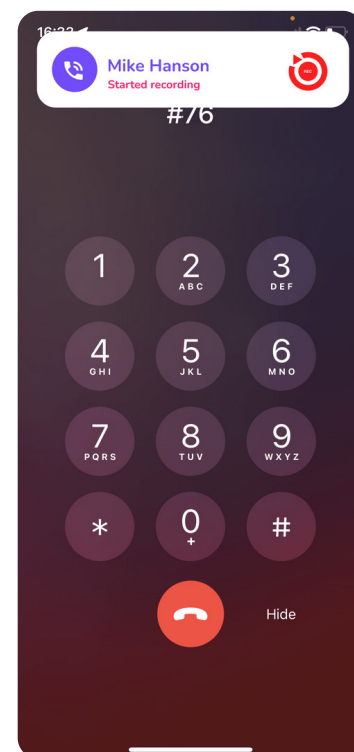
Secure Cloud Storage with Role-Based Access

Every call made through PiPcall is:

- Stored securely in the cloud
- Time-stamped
- Accessible via a central admin dashboard
- Retained for at least 90 days — or longer for flagged incidents

Only authorised team members can access recordings, supporting both day-to-day audits and post-incident investigations.

This meets and simplifies compliance with NR/L3/OPS/301/05's strict requirements around evidence protection, access control, and auditability.
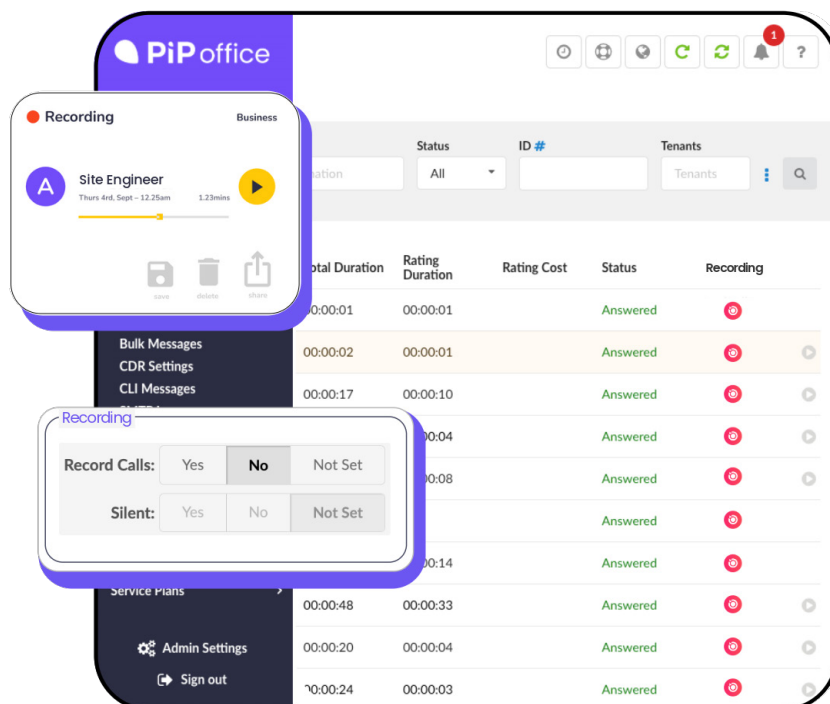
Seamless Rollout to Contractors, Subcontractors and Umbrella Workers

One of PiPcall's biggest advantages? It doesn't require new hardware or fixed lines. You can deploy it:

- On personal phones (BYOD) or company devices
- To contractors working under multiple entities
- Without SIM swaps or long provisioning lead times

That means every COSS, PICOP, MOM, ES, and supervisor can be compliant within hours, not weeks.

Built-in Admin Tools for Rail Teams

PiPcall gives operations managers and compliance leads a centralised platform to:

- Assign numbers or shared lines (e.g., for supervisor teams)
- Monitor live calls
- Assign and manage eSIMs
- Control access and retention policies
- Instantly retrieve call data for CRGs or safety reviews

It's a single pane of glass — with no IT overload and no change management headaches.

The PiPcall Advantage, at a Glance

Feature	PiPcall		Traditional Setup	
Call recording	Recorded centrally over the Mobile Voice Network	✅	VoIP app or no recording available	❌
Central cloud storage	Stored in the secure PiPcall Portal	✅	Device-based or siloed	❌
BYOD compatibility	Easy onboarding and zero cost to the user	✅	Requires workaround	❌
Role-based access	Compliant control	✅	No admin visibility	❌
Deployment speed	Same-day	✅	Weeks/months	❌
Rail-aligned compliance	NR/L3/OPS/301-ready	✅	Partial or non-compliant	❌

Chapter 6: Compliance Toolkit for Decision Makers

Your practical guide to mobile call recording readiness in the UK rail industry.

Why You Need a Toolkit

As a safety, operations, or IT leader in the rail sector, you're facing increasing responsibility for communication compliance — not just internally, but across every link in your workforce: contractors, subcontractors, and umbrella staff.

This chapter provides a simple set of questions and tools to assess whether your organisation is ready to meet the expectations outlined in NR/L3/OPS/301.

Use it to identify risks, align stakeholders, and plan your next steps — before an incident forces you to.

Mobile Compliance Checklist

Answer these 10 yes/no questions. If you answer "no" to any, you may have a compliance gap.

Question	Yes / No
1. Can you record mobile calls automatically?	
2. Are calls recorded even when users have no access to Wi-Fi (e.g., rural track)?	
3. Can you store call recordings securely in the cloud?	
4. Are recordings retained for at least 90 days — or longer if related to an incident?	
5. Can authorised investigators retrieve recordings within 24 hours of an event?	
6. Are you recording calls from contractors, subcontractors, and umbrella workers?	
7. Is your system compatible with BYOD (Bring Your Own Device) policies?	
8. Can admin teams assign, monitor, and revoke access from a central dashboard?	
9. Are recordings protected from deletion, tampering, or unauthorised access?	
10. Are your Communication Review Groups able to access and assess call data?	

Score 8–10 "Yes" answers: You're in strong shape — but still review scenarios for edge cases.
 Score 5–7: Moderate risk — begin closing gaps, especially around subcontractor workflows.
Score below 5: High risk — action needed to avoid regulatory or safety exposure.

Team Roles & Responsibilities Matrix

Ops Managers: Ensure all staff have compliant tools and workflows

Safety Leads: Lead SCC training, investigation support, and audits

IT Admins: Deploy and manage mobile compliance tools (e.g., PiPcall)

Contractor Managers: Confirm third-party workers are fully compliant

CRG Chairs: Review calls, lead quarterly assessments, and enforce action items

What You Should Do Next

1. **Map your mobile workflows:** Document who is using what device, under what conditions, and whether those calls are recorded.

2. **Identify any unrecorded communications:** Are contractors using personal phones? Are supervisors outside GSM-R coverage?

3. **Review current tools vs. regulatory needs:** Compare your system to NR/L3/OPS/301 recording, storage, access, and retention standards.

4. **Book a compliance consultation:** Let PiPcall help you benchmark and design a rollout plan that fits your team size, contractor network, and safety culture.

PiPcall: A Ready-to-Deploy Toolkit

PiPcall isn't just an app — it's a complete compliance platform for mobile teams:

- Built for rail sector complexity
- Compatible with company-issued and personal mobiles
- Enforces recording across every call
- Makes CRG reporting, incident review, and audit response simple

Chapter 7: Proactive Compliance = Safer Rail

Why communication strategy is now a safety strategy.

Rail Has Changed — And So Has Responsibility

Today's UK rail environment is more mobile, decentralised, and partnership-driven than ever. But with that flexibility comes risk — especially when it comes to critical communications.

The Network Rail regulations laid out in NR/L3/OPS/301 and NR/L2/TEL/30002 aren't just another layer of bureaucracy. They reflect a wider industry shift toward:

• Clearer responsibility across organisational boundaries
• Faster, more transparent investigations
• Accountability for contractors and subcontractors
• Evidence-based safety performance

And at the heart of all these goals is one thing: verbal communication — captured, stored, and managed correctly.

Reactive Isn't Enough Anymore

Waiting until an incident happens to ask "Was that call recorded?" or "Who made the decision?" is no longer acceptable. A reactive approach exposes you to:

• Regulatory violations
• Delays in incident resolution
• Legal disputes or liability
• Loss of stakeholder trust

A proactive approach, on the other hand, gives you:

• Clarity under pressure
• Faster investigation cycles
• Better training and performance reviews
• Stronger contractor oversight
• Proof of safety leadership

Safety Culture Starts with Communication Culture

Think of every mobile call not as a side channel — but as a core operational asset.

By embedding compliance-grade recording and monitoring into everyday mobile workflows, you don't just protect the business. You support the people making the calls.

That includes:

- The MOM racing to an infrastructure fault
- The COSS giving line block instructions
- The investigator reconstructing an hour-by-hour timeline
- The control centre team ensuring trains stay moving — and safe

PiPcall: Compliance That Works in the Field

PiPcall gives your team:

- One mobile platform that works with any device, any team, any scale
- Mobile Voice Network calls initiated via app; recording handled centrally by PiPcall's system
- Recordings stored securely in the PiPcall Portal, not on the device (aligned with rail regulations).
- Admin tools that support everyone — from safety leads to IT teams
- It's not just mobile. It's mobile built for rail.

Let's Get You Ready
Whether you're responsible for safety, operations, or technology — if you want to close compliance gaps and stay ahead of changing expectations, now is the time to act.

Let us help you:
- Map your mobile exposure
- Assess your current risk level
- Create a rollout plan tailored to your network, team, and devices

Start Today.
We're here to support your journey to safer, smarter mobile compliance.

Phone: 0330 094 8080
Email: sales@pipcall.com