



RingRx Communication Guides

Phishing Attempts (Calls)

Practical tips to help your healthcare team communicate with confidence.

What This Is For

Help your team handle suspicious calls in a calm, consistent, and secure way.

Use This When

- ✓ A caller asks for sensitive patient or account information
- ✓ A caller claims urgency and pressures staff to act quickly
- ✓ A third party cannot be verified but requests details or access

Customization Guidance

- ✓ **Use your practice's standard verification** process before discussing any patient or account details
- ✓ **Route unusual or high-pressure requests** to a manager or designated contact
- ✓ **Do not rely** on caller ID alone to verify identity
- ✓ **If the caller claims** to represent a vendor, payer, or partner, confirm through a known callback number
- ✓ **Document the call** and what was requested before moving on

Do

- ✓ Use a calm, steady pace
- ✓ Take ownership of the next step
- ✓ Collect only the minimum information needed for follow-up
- ✓ Report the call internally

Don't

- ✗ Share patient, billing, or staff information without verification
- ✗ Confirm names, dates of birth, account details, or schedules
- ✗ Stay on the call to debate the request
- ✗ Let urgency override your process

Recommended Script

I'm not able to verify or share that information on this call.

If you need assistance, I can take your name, organization, and callback number and pass this to the appropriate person for review.

I'm not able to go further until that review is complete.



Tone Tip

Be calm and brief. Do not argue or explain more than necessary.

HIPAA Reminder

Confirm the patient's identity before discussing details. Avoid leaving detailed information in voicemails or texts.

RingRx Tip

Use call logs to document suspicious calls and support internal follow-up.

Review Note

Review quarterly or when staffing responsibilities or escalation policies change.