Medical Practice Compliance Checklist

A Practical Self-Assessment for Independent & Group Practices

Compliance Series

This checklist was developed from direct operational experience running a multi-specialty women's health platform in North Fulton County, Georgia. Use it quarterly and after any significant operational change to identify gaps before they become enforcement actions, audits, or accreditation failures.

> ***Why this matters now: CMS, OIG, and state medical boards have significantly increased audit activity targeting independent practices. A single HIPAA breach can cost $100K–$1.9M per violation category. Anti-Kickback violations carry criminal exposure. Most practices have correctable gaps — the question is whether you find them first.***

1. HIPAA Privacy & Security

Notice of Privacy Practices (NPP) posted and provided to new patients	■ Met ■ Gap ■ N/A	_____
Business Associate Agreements (BAAs) in place with all PHI-handling vendors (EHR, billing, lab, IT)	■ Met ■ Gap ■ N/A	_____
Annual HIPAA training completed and documented for all staff	■ Met ■ Gap ■ N/A	_____
Designated HIPAA Privacy Officer identified and documented	■ Met ■ Gap ■ N/A	_____
Security Risk Analysis (SRA) completed within the last 12 months	■ Met ■ Gap ■ N/A	_____
Breach notification policies written, tested, and within 60-day reporting window	■ Met ■ Gap ■ N/A	_____
Minimum Necessary standard applied to all PHI disclosures	■ Met ■ Gap ■ N/A	_____
Patient right-of-access requests fulfilled within 30 days — process documented	■ Met ■ Gap ■ N/A	_____
Texting/email/portal communications reviewed for PHI exposure	■ Met ■ Gap ■ N/A	_____
Workforce sanctions policy exists for HIPAA violations	■ Met ■ Gap ■ N/A	_____

> ***Note: The OCR 'Right of Access' initiative has resulted in settlements for practices as small as single-physician offices. Timeliness is the #1 audit trigger.***

2. Medical Billing, Coding & Revenue Cycle

Superbills and charge capture reviewed against current CPT/ICD-10 code sets annually	■ Met ■ Gap ■ N/A	_____
E&M; documentation supports level billed (audit 10 random charts per provider)	■ Met ■ Gap ■ N/A	_____
Modifier usage reviewed — 25, 59, 51 and others used correctly and consistently	■ Met ■ Gap ■ N/A	_____
No unbundling of procedures that should be billed under a single code	■ Met ■ Gap ■ N/A	_____
Provider enrollment and credentialing current with all active payers	■ Met ■ Gap ■ N/A	_____
Claims denial rate tracked monthly; root cause analysis on high-volume denials	■ Met ■ Gap ■ N/A	_____
Advance Beneficiary Notices (ABNs) obtained and retained for Medicare patients	■ Met ■ Gap ■ N/A	_____
No routine waiving of copays or deductibles as policy	■ Met ■ Gap ■ N/A	_____
Incident-to billing rules followed correctly for mid-level providers	■ Met ■ Gap ■ N/A	_____
Internal billing audit completed within the past 12 months	■ Met ■ Gap ■ N/A	_____
Overpayment refund process exists; refunds issued within 60 days of identification	■ Met ■ Gap ■ N/A	_____

> ***Note: Incident-to billing for APRNs and PAs is one of the most frequently misapplied rules in outpatient OB/GYN. Incorrect use is False Claims Act exposure — not merely a billing error.***

3. Corporate Structure, Stark Law & Anti-Kickback

All physician compensation arrangements reviewed for Fair Market Value (FMV) compliance	■ Met ■ Gap ■ N/A	_____
No percentage-of-revenue compensation arrangements with referral sources	■ Met ■ Gap ■ N/A	_____
Space/equipment leases with other providers meet safe harbor requirements (FMV, written, ≥1 yr)	■ Met ■ Gap ■ N/A	_____
Management service agreements with non-physician entities reviewed by healthcare counsel	■ Met ■ Gap ■ N/A	_____
Ownership interests in entities that receive referrals are disclosed and documented	■ Met ■ Gap ■ N/A	_____
Employed provider contracts reviewed for Stark II Phase III compliance	■ Met ■ Gap ■ N/A	_____
No arrangements constituting improper remuneration to patients	■ Met ■ Gap ■ N/A	_____
State corporate practice of medicine laws reviewed (Georgia-specific requirements verified)	■ Met ■ Gap ■ N/A	_____

Note: Any MSO, billing, or management agreement with a third party must be reviewed by a healthcare transactions attorney — not a general business attorney. This is non-negotiable.

4. Provider Credentialing & Privileging

All providers credentialed with each payer where they see patients	■ Met ■ Gap ■ N/A	_____
Hospital privileges current and in good standing for all applicable providers	■ Met ■ Gap ■ N/A	_____

DEA registration current for all providers prescribing controlled substances	■ Met ■ Gap ■ N/A	_____
Georgia Composite Medical Board license current; renewal dates calendared	■ Met ■ Gap ■ N/A	_____
APRN/PA supervisory agreements in writing and filed appropriately	■ Met ■ Gap ■ N/A	_____
CAQH profiles updated within the last 90 days	■ Met ■ Gap ■ N/A	_____
Malpractice insurance certificates current; nose/tail coverage evaluated on transitions	■ Met ■ Gap ■ N/A	_____
Credentialing files maintained for minimum 7 years post-employment	■ Met ■ Gap ■ N/A	_____

5. Employment, HR & Labor Compliance

All staff correctly classified as employees vs. independent contractors (IRS 20-factor test)	■ Met ■ Gap ■ N/A	_____
Employee handbook current; reviewed by employment counsel within last 2 years	■ Met ■ Gap ■ N/A	_____
I-9 forms completed and retained for all employees	■ Met ■ Gap ■ N/A	_____
OSHA Bloodborne Pathogen training completed and documented annually	■ Met ■ Gap ■ N/A	_____
Workplace violence prevention policy in place	■ Met ■ Gap ■ N/A	_____
Non-competes reviewed for Georgia enforceability (O.C.G.A. § 13-8-50 et seq.)	■ Met ■ Gap ■ N/A	_____
Provider employment agreements include clear tail coverage and post-termination obligations	■ Met ■ Gap ■ N/A	_____
Performance documentation process consistent and legally defensible	■ Met ■ Gap ■ N/A	_____

6. Clinical Operations & Patient Safety

Emergency protocols documented, posted, and staff trained (anaphylaxis, OB emergency, cardiac)	■ Met ■ Gap ■ N/A	_____
Crash cart and emergency medications checked and logged monthly	■ Met ■ Gap ■ N/A	_____
Medication storage, labeling, and controlled substance logs comply with DEA requirements	■ Met ■ Gap ■ N/A	_____
Adverse event and near-miss reporting process exists and is consistently used	■ Met ■ Gap ■ N/A	_____
No copy-forward documentation without individualized attestation	■ Met ■ Gap ■ N/A	_____
Informed consent process documented in writing for all procedures	■ Met ■ Gap ■ N/A	_____
After-hours coverage arrangement documented and communicated to patients	■ Met ■ Gap ■ N/A	_____
Referral tracking system in place to confirm receipt and provider response	■ Met ■ Gap ■ N/A	_____

7. Technology, Cybersecurity & EHR

EHR access reviewed; terminated employees removed within 24 hours of separation	■ Met ■ Gap ■ N/A	_____
Multi-factor authentication (MFA) enabled on all clinical and billing platforms	■ Met ■ Gap ■ N/A	_____
Regular data backups performed and tested; off-site or cloud backup verified	■ Met ■ Gap ■ N/A	_____

Ransomware response plan documented and communicated to staff	■ Met ■ Gap ■ N/A	_____
Business Associate Agreement in place with EHR vendor	■ Met ■ Gap ■ N/A	_____
Audit logs reviewed periodically for unusual access patterns	■ Met ■ Gap ■ N/A	_____
Patient portal communications reviewed for PHI security	■ Met ■ Gap ■ N/A	_____
IT vendor access to PHI documented and limited to minimum necessary	■ Met ■ Gap ■ N/A	_____

Scoring & Next Steps

0–3 gaps	Low	Maintain cadence; schedule next review in 6 months
4–8 gaps	Moderate	Prioritize Sections 1–3; engage compliance advisor
9–15 gaps	High	Immediate remediation plan required; consider external compliance support
15+ gaps	Critical	Engage a healthcare compliance attorney and MSO partner immediately

Ready for a no-obligation compliance review? HURF Healthcare Associates and HURF Accounting & Business Solutions offer a complimentary 30-minute Practice Health Assessment for qualifying independent practices. Our team has operated a multi-specialty OB/GYN and women's health platform in North Fulton County — we understand the real operational pressures you face. **Schedule your assessment: hurfhealthcare.com/consult**