Epic Security Build Reference Guide

Templates | HIPAA | Audit Log | Break-Glass | TechFitFlow.com

Design templates around job function, not job title. Use base template + SubTemplate model to control proliferation. Every template requires privacy officer minimum necessary sign-off before production.

SECTION 1 - SECURITY TEMPLATE DESIGN PRINCIPLES

Design by job function, not job title	A single "Nurse" template is always wrong. ICU RN, ED RN, clinic RN, and agency RN have different workflow requirements and different appropriate access scopes. Template must match the specific workflow performed, not the professional credential held.
Start from minimum, add up - never copy down	Always start from the minimum access template and add required permissions. Never copy an existing template and remove items. Copied templates inherit access that may exceed minimum necessary for the new role. The inherited access is invisible without careful comparison.
Base template + SubTemplate model	One base template per broad role category (RN, MD, Pharmacist, Registrar). SubTemplates add department-specific or specialty-specific capabilities. Users get base + applicable SubTemplates. This limits total template count while accommodating legitimate variation.
Privacy officer review before production	Every template - new or modified - requires documented privacy officer minimum necessary review before assignment to any production user. Review confirms each access right is justified by the specific job function. Unsigned templates do not go to production.
Template change control	Every modification to a security template requires a change request with: what changed, why it changed, who approved, and when it took effect. This documentation is the audit artifact for any future investigation of access decisions.
Annual re-certification	Every active template must be re-certified annually against current job function descriptions from HR. Supervisors sign off that their staff's template still matches what those staff members actually do. Unsigned re-certifications result in account suspension after 30-day notice.

SECTION 2 - SENSITIVE RECORD CLASS CONFIGURATION

Record Type	Regulatory Basis	Epic Mechanism	Who Gets Access	Audit Requirement
Behavioral Health	HIPAA + state law	Sensitivity flag; restricted security class	BH staff + treating providers + BH-credentialed care coordinators	Every access logged; break-glass required for out-of-dept access; privacy officer notified
SUD (42 CFR Part 2)	42 CFR Part 2	42 CFR Part 2 module; consent tracking	SUD treatment providers only; patient consent required for disclosure	Consent log required; disclosure log required; no disclosure without specific patient consent

HIV/AIDS	State law (varies)	Sensitivity flag; diagnosis masking	Treating provider; ID dept; lab for results only	Elevated monitoring per state; access log reviewed monthly for non-treating access
VIP/Confidential	HIPAA; org policy	VIP flag; treating team restriction	Directly assigned treating team only - no general clinical staff access	All access logged; privacy officer immediate notification of any non-treating access
Genetic Information	GINA; HIPAA	Sensitivity flag; restricted to ordering provider	Ordering provider; genetics counselor; lab	Standard HIPAA audit; data cannot be used for employment or insurance decisions

SECTION 3 - BREAK-GLASS CONFIGURATION REQUIREMENTS

	Break-Glass Requirement
[ ]	Override prompt is visible and mandatory - user must provide a reason before the restricted record opens
[ ]	Override prompt cannot be skipped, minimized, or auto-populated - user must actively type or select a reason
[ ]	Break-glass event triggers immediate notification to privacy officer or security team - not a daily batch report
[ ]	Audit log entry captures: user ID, patient ID, timestamp, stated reason, workstation - all fields required
[ ]	Privacy officer reviews every break-glass event within 24 hours and documents review outcome
[ ]	Pattern monitoring: any user who invokes break-glass more than twice in a week is flagged for privacy officer review
[ ]	Break-glass is not a solution to incorrect template design - frequent break-glass for routine work = template problem
[ ]	Quarterly break-glass report reviewed by privacy officer and department leadership jointly