

Epic Security Build - Go-Live Readiness Checklist

Templates | Provisioning | Audit Log | HIPAA | TechFitFlow.com

Every gate requires a named owner and documented sign-off before go-live. Temporary go-live access grants must have documented expiration dates. Post-go-live access cleanup must be scheduled within 30 days.

SECURITY TEMPLATE REVIEW AND SIGN-OFF

	Gate Item	Owner	Sign-off
[]	All production security templates have been reviewed by the security analyst against job function descriptions	_____	_____
[]	Privacy officer has signed off on every template confirming minimum necessary access is appropriate	_____	_____
[]	No Epic sample templates deployed unreviewed - all have been customized for org workflow and access scope	_____	_____
[]	Template inventory documented: name, role category, workflow it supports, modules included, user count	_____	_____
[]	SubTemplate inventory documented: what each SubTemplate adds and which base templates it attaches to	_____	_____
[]	Sensitive record class configuration reviewed: behavioral health, SUD, VIP, HIV sensitivity flags confirmed	_____	_____
[]	Template testing completed: test user with each template confirmed - can do required actions, cannot do restricted actions	_____	_____
[]	Template change control process documented and communicated to IT security team before go-live	_____	_____

BREAK-GLASS CONFIGURATION

	Gate Item	Owner	Sign-off
[]	Break-glass override prompt configured - user must actively provide a reason before restricted record opens	_____	_____
[]	Override prompt cannot be auto-populated or skipped - confirmed in test environment	_____	_____
[]	Break-glass notification configured - privacy officer receives immediate notification of every override event	_____	_____
[]	Audit log entry for break-glass captures: user, patient, timestamp, reason, workstation - all fields populated	_____	_____
[]	Break-glass tested end-to-end: triggered override, confirmed notification received by privacy officer, confirmed audit log entry	_____	_____

	Gate Item	Owner	Sign-off
[]	Pattern monitoring configured: automated flag if any user invokes break-glass more than twice in a week	_____	_____
[]	Privacy officer review process documented for break-glass events: review within 24 hours, outcome documented	_____	_____

USER PROVISIONING PROCESS VALIDATION

	Gate Item	Owner	Sign-off
[]	Job-function-to-template mapping table documented: every role maps to a specific base template and optional SubTemplates	_____	_____
[]	Supervisor approval step confirmed in provisioning workflow - no account created without supervisor sign-off	_____	_____
[]	Provisioning SLA defined: account ready before employee's first shift	_____	_____
[]	Provisioning request form includes: job title, department, supervisor name, start date, and specific template requested	_____	_____
[]	Access request form template created and distributed to hiring managers before go-live	_____	_____
[]	IT security team trained on provisioning process and mapping table - no ad hoc template assignments	_____	_____
[]	Go-live access grants documented with expiration dates: all temporary IT/analyst elevated access expires within 60 days	_____	_____

DEPROVISIONING PROCESS VALIDATION

	Gate Item	Owner	Sign-off
[]	HR-to-Epic integration configured for automatic account suspension on termination (if available)	_____	_____
[]	If manual: deprovisioning SLA documented as 24 hours from last day - named owner responsible for each step	_____	_____
[]	Escalation path documented for missed deprovisioning SLA: who is notified, within what timeframe	_____	_____
[]	Leave of absence account suspension process documented: accounts suspended within 5 business days of leave start	_____	_____
[]	Role change process documented: old template removed and new template assigned before start of new role	_____	_____
[]	Weekly audit process established: active Epic accounts compared to current HR records - remediation within 24 hours	_____	_____
[]	Termination notification chain from HR to IT documented and tested with at least one test scenario	_____	_____

AUDIT LOG AND MONITORING PROGRAM

	Gate Item	Owner	Sign-off
[]	Epic audit log confirmed collecting: user ID, patient ID, action, timestamp, workstation for all PHI access	_____	_____
[]	Audit log extraction to Clarity confirmed - logs available for Reporting Workbench query	_____	_____
[]	Privacy officer named as audit log review owner with documented review frequency (minimum weekly)	_____	_____
[]	Audit log review process documented: what patterns are reviewed, how anomalies are escalated, within what timeframe	_____	_____
[]	VIP/confidential patient monitoring configured: all chart accesses flagged for privacy officer review	_____	_____
[]	Out-of-department access monitoring configured: accesses by users outside primary department flagged weekly	_____	_____
[]	Break-glass audit review scheduled: all events reviewed within 24 hours, quarterly summary to leadership	_____	_____
[]	Annual audit log review cycle established: full year of logs reviewed before annual compliance attestation	_____	_____
[]	Post-go-live access cleanup scheduled within 30 days: all go-live temporary access grants reviewed and revoked or formalized	_____	_____