BUILDING A CULTURE OF PRIVACY & SECURITY

Organizational Strategies by Level

ABOUT THESE STRATEGIES

This chart outlines strategies for fostering a strong culture of privacy and security throughout an HMIS ecosystem. Each organizational level plays a role in reinforcing values, behaviors, and practices that protect sensitive data and support compliance.

Level	Culture Strategy	Examples
Leadership	Visibly support and communicate the value of data privacy and security as an organizational priority	CEO sends quarterly message on data integrity; security update included in board reports
Legal Council	Provide legal guidance on data use, sharing, and retention; ensure compliance with applicable laws and contracts	Ensure legal compliance by reviewing and interpreting data sharing agreements, privacy laws, and regulatory guidance.
Privacy Officer	Oversees compliance with privacy regulations and guides policy and incident response efforts	Coordinates policy reviews, supports breach response, advises on data-sharing risks and safeguards
System Administrators	Builds technical safeguards and automates enforcement of policies	Role-based access enforced in system configuration; login attempts and exports monitored routinely
Governance Bodies	Makes security/privacy a standing topic in governance and planning discussions	Includes audit results in HMIS Committee meetings; review user agreement revisions annually
Agency Admins	Monitor access and data use across users; reinforce best practices during regular team touchpoints	Weekly checks of logins/exports; team reminders to verify client consent before sharing data
Program Management	Integrate privacy into operational planning, training expectations, and performance reviews	Supervisors check on timely role removals during offboarding; track staff training completions
Frontline Staff	Embed privacy and security into daily workflows and encourage question-asking and peer accountability	Case managers flag incorrect visibility settings; peer reminders to lock screens when away
Training Teams	Offer relevant, engaging training tailored to different roles and reinforce over time	Short monthly videos or quizzes; scenario-based refreshers by user type
Communications	Normalize regular, approachable messaging about privacy and data use	“Security Tip of the Month” email, Slack reminders, or shout-outs for strong stewardship