

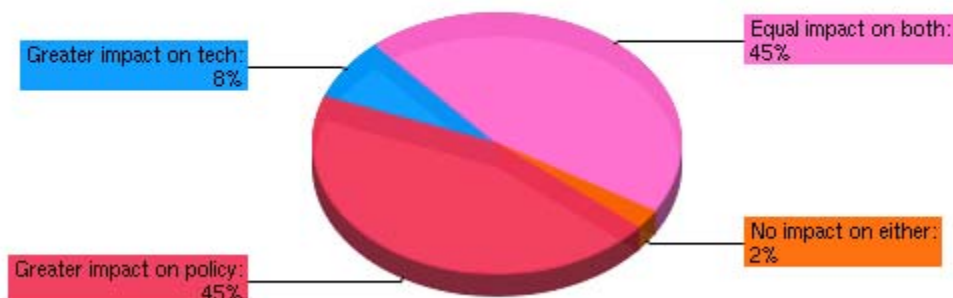
Results: 2011 Health IT, HIPAA & Security Survey

Statistics

Total Responses from Qualified IT Professionals at Healthcare Provider Organizations

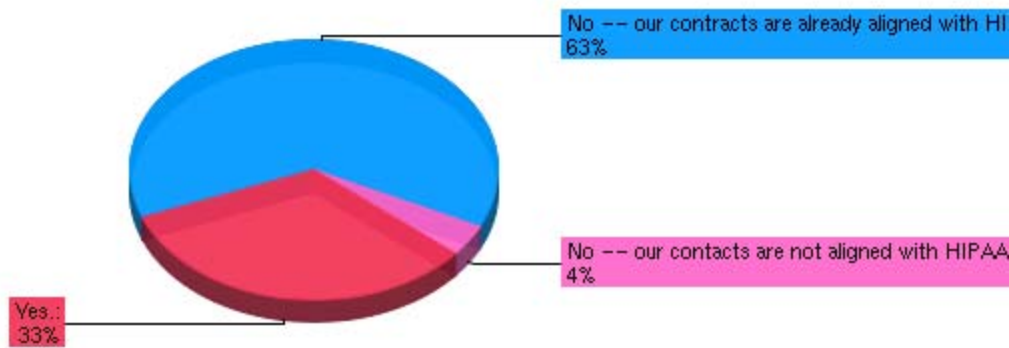
255

Do HIPAA mandates have greater impact on your security policies or tech purchases?



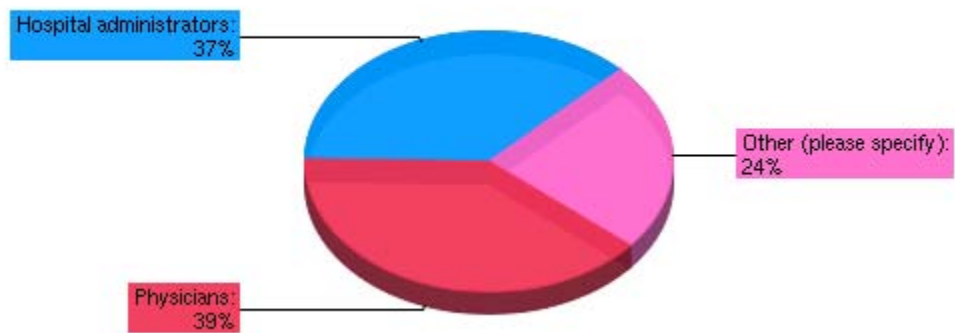
Value	Count	Percent %
Greater impact on policy	114	44.7%
Greater impact on tech	20	7.8%
Equal impact on both	115	45.1%
No impact on either	6	2.4%

Are you planning to update business associate and third-party vendor contracts in the next two years to reflect HIPAA rules?



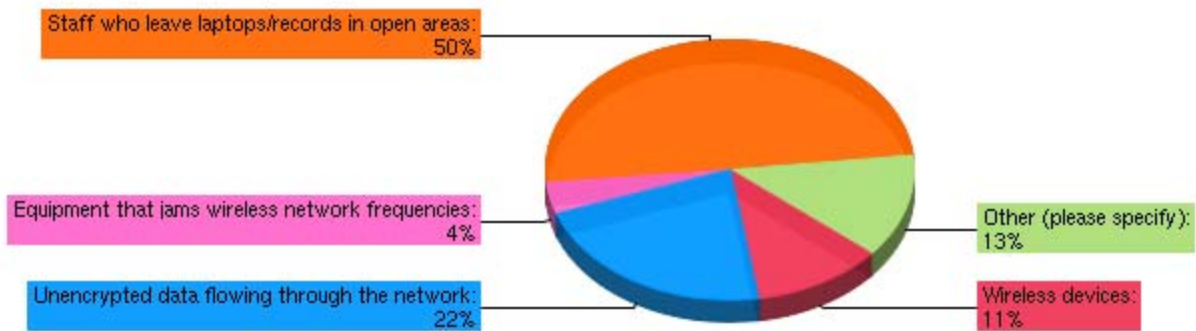
Value	Count	Percent %
Yes.	84	32.9%
No -- our contracts are already aligned with HIPAA considerations.	161	63.1%
No -- our contacts are not aligned with HIPAA but we'll align them later.	10	3.9%

Who is the biggest influence on whether and how point-of-care wireless devices are used in your hospital?



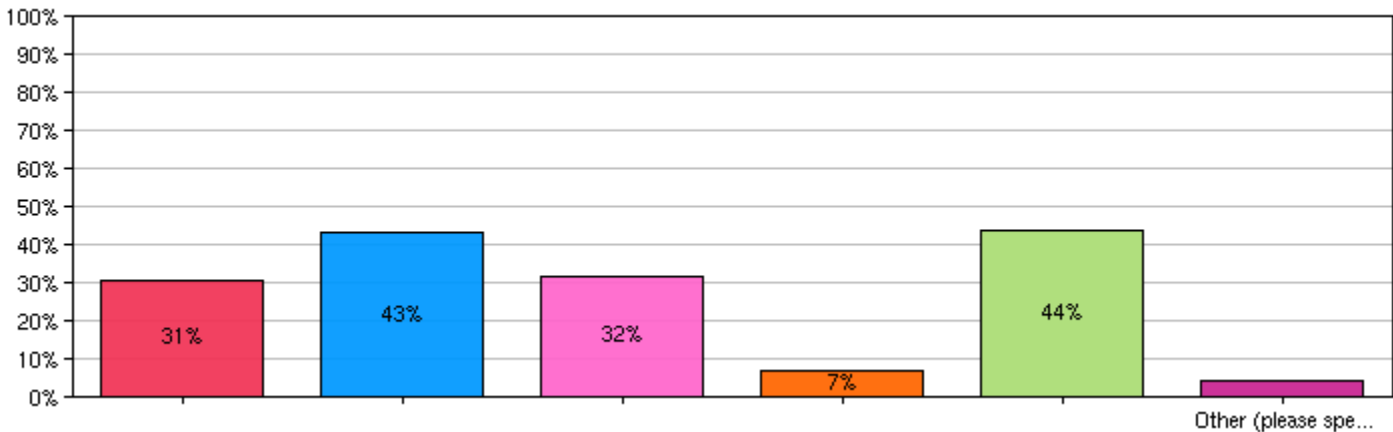
Value	Count	Percent %
Physicians	100	39.2%
Hospital administrators	95	37.3%
Other	60	23.5%

What is the weakest link in your hospital's security?



Value	Count	Percent %
Wireless devices	29	11.4%
Unencrypted data flowing through the network	56	22%
Equipment that jams wireless network frequencies	10	3.9%
Staff who leave laptops/records in open areas	127	49.8%
Other	33	12.9%

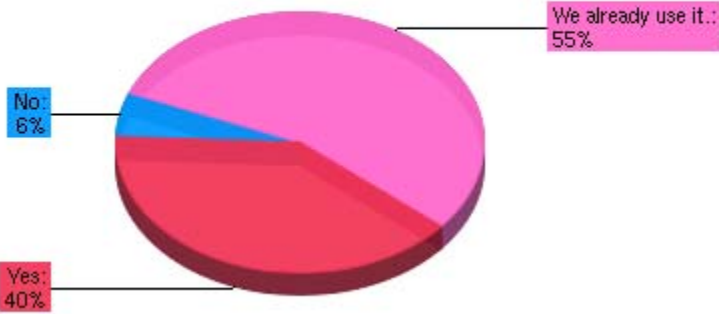
What are you doing to secure your hospital's wireless network?
(Check all that apply)



Value	Count	Percent %
Partitioning it so patient data is separate from everything else.	78	30.6%
Strengthening the authentication necessary to access clinical applications.	110	43.1%
Replacing WEP encryption with more robust WPA encryption.	81	31.8%
We do not have a wireless network.	18	7.1%
We have already fully secured our wireless network.	111	43.5%

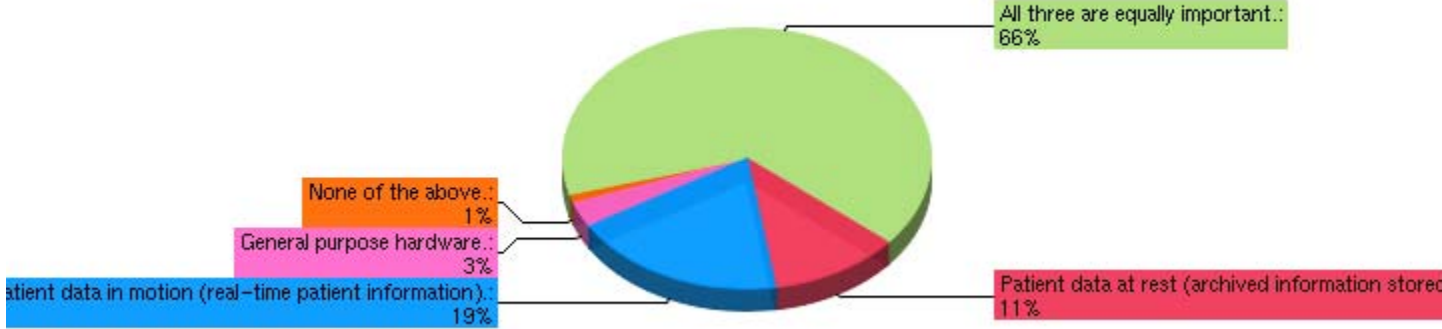
Other	11	4.3%
-------	----	------

HIPAA enforcement authorities have said that when encrypted patient data is lost, it doesn't count as a data breach and therefore is not a violation. Will this make your organization more likely explore encryption software for patient data?



Value	Count	Percent %
Yes.	101	39.6%
No.	14	5.5%
We already use it.	140	54.9%

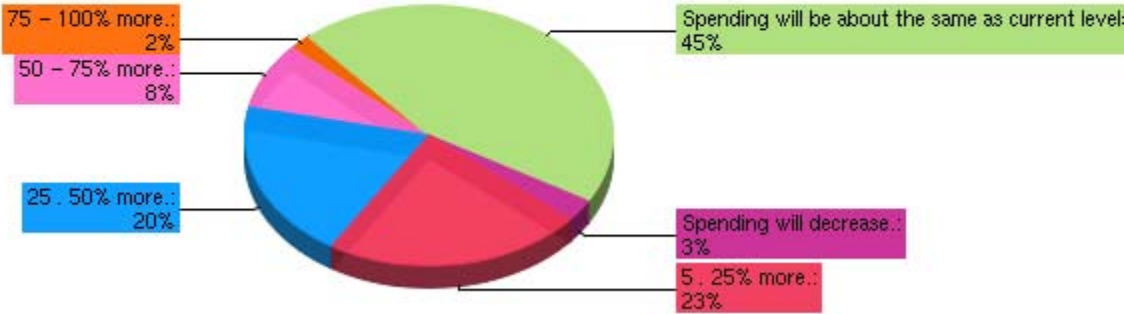
What is most important for you to encrypt?



Value	Count	Percent %
Patient data at rest (archived information stored in EHRs, PACS or other systems).	29	11.4%
Patient data in motion (real-time patient information).	48	18.8%

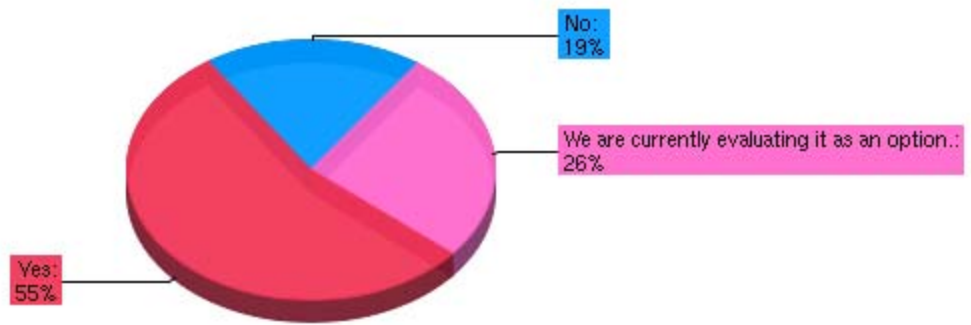
General purpose hardware.	8	3.1%
None of the above.	3	1.2%
All three are equally important.	167	65.5%

Are you planning to spend more or less on clinical data encryption in the next two years?



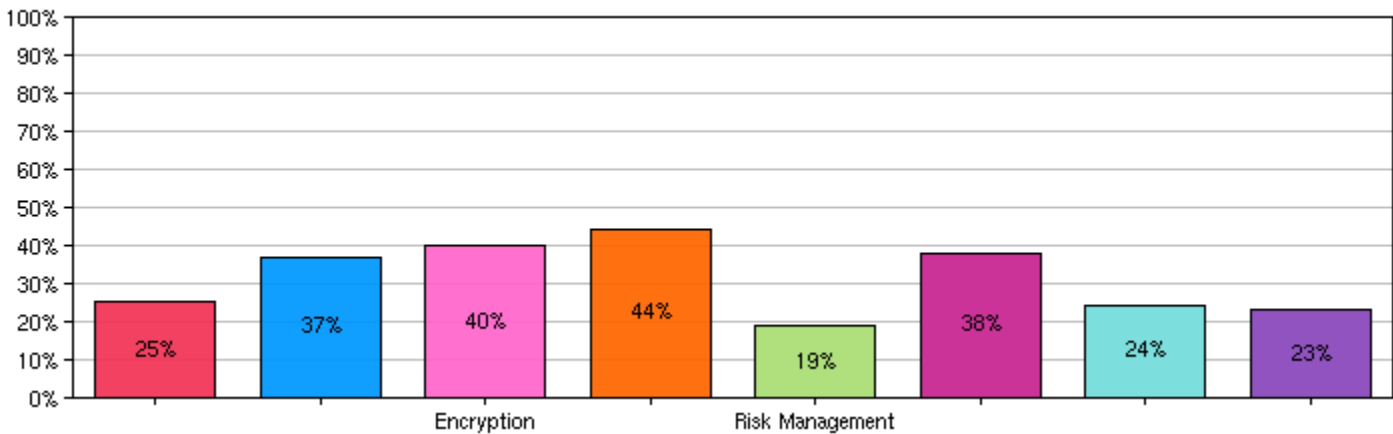
Value	Count	Percent %
5 - 25% more.	58	22.7%
25 - 50% more.	50	19.6%
50 - 75% more.	21	8.2%
75 - 100% more.	5	2%
Spending will be about the same as current levels.	114	44.7%
Spending will decrease.	7	2.7%

Do single sign-on applications play a significant role in your user authentication practices?



Value	Count	Percent %
Yes	139	54.5%
No	49	19.2%
We are currently evaluating it as an option.	67	26.3%

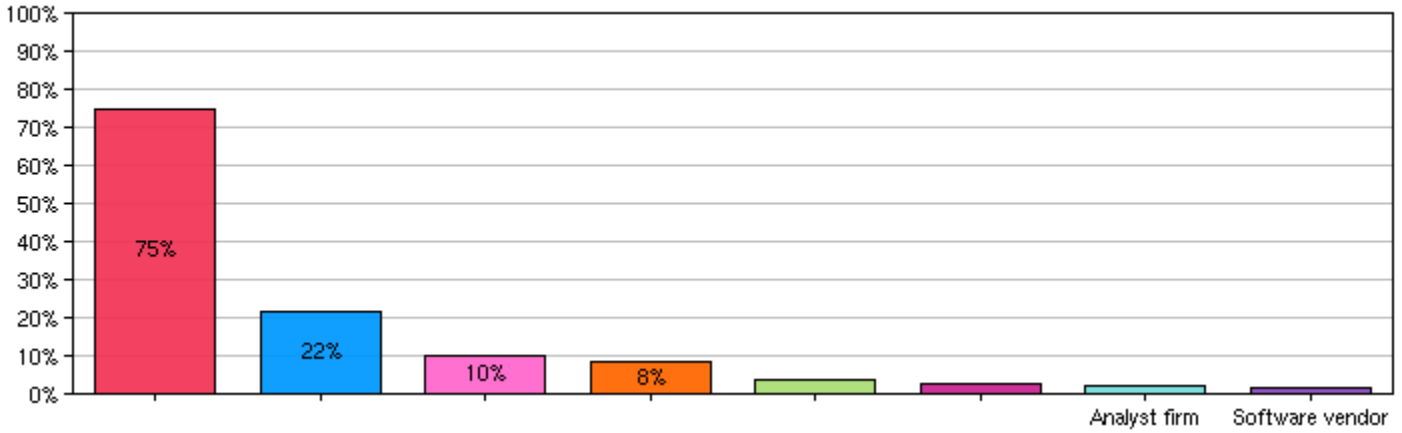
Which of the following technologies do you plan to purchase in the next 6-12 months to help your organization achieve HIPAA compliance? (Check all that apply)



Value	Count	Percent %
Data Loss Prevention	64	25.1%
Data Backup/Storage	94	36.9%
Encryption	102	40%
Mobile Device Security	113	44.3%
Risk Management	48	18.8%
User Authentication/ID and Access Management	97	38%

Vulnerability Management and Assessment	62	24.3%
Wireless Network Security	59	23.1%

What best describes your organization/company?



Value	Count	Percent %
Ambulatory care facility, outpatient center, large group physician practice or home health care	54	21.6%
Ancillary clinical service provider	21	8.2%
Federal, state or municipal health agency	25	9.8%
Hospital, medical center, multi-hospital system or IDN	190	74.9%