**Understanding IT Security and Compliance**

All users who access systems which contain patient information have an important role in the organization. As health care data continues to enter the electronic age, so do the threats against the systems and users of this precious information. As the FBI explained to a group, I attended in DC this winter explained, “it is not if you will be breached, but when”. The agencies which govern healthcare information understand that there is no single solution to stop these threats from happening. It is up to the departments that manage the information and its infrastructure to maintain proper procedure and method in order to safeguard against such threats.

Your IT department plays a critical role in this area. Companies who have had the most significant breaches of data in the past have paid millions in fines which most of the time is not covered entirely by insurance leaving the organization to cover these costs or close their doors. This is often a result of poor procedures and housekeeping internally, which would have almost eliminated the fines all together, by proving they acted in accordance with policy supported by HIPAA, NIST, OCR and other agency recommendations.

While the IT requirements to perform any changes or modifications in the system may seem unreasonable, it is never personal. It is merely to ensure that every action we perform has proper documentation and approval. This is to protect the company and those who work within it. All systems in the organization have access to sensitive information which must be protected at all costs.

It may seem like a trivial request at times but having proper documentation and procedure will save the organization if an incident ever occurs. IT will always prepare for worst case scenarios in order to try and foresee what is possible and negate any such possibilities.

Please be patient with your IT professionals when asked to perform tasks which seem like extra steps. Asking for records or emails to originate from the requestor is a basic way we record change control, as having a technician create his or her own tickets completely removes all credibility of any change.

It is all of our responsibility to ensure that the company, and the patient information it houses, is protected at all times. IT is held to strict process and policy in order to ensure that every possible step is taken at all times to ensure data integrity and safety.

If anyone has questions or comments, I am always available directly and would be happy to assist in any manner I can.

Sincerely,

*Edward Dibeler*
*CEO*
Puma Telecommunications
ed@pumatelecommunications.com