Participant Information Protection & Confidentiality in RadComp



With ever growing concerns over the privacy personal information, we want to assure you RadComp is taking every precaution to secure and protect participant data. The RadComp Study adheres to strict federal regulations that require all information that can identify a participant to be kept confidential, as per Good Clinical Practice guidelines. Much of the following information has been previously detailed, by law, to each participant when first joining the study during the Informed Consent process.

Why is participant contact and health information used?

Participant's information is used by the research team to contact participants during the study. This information and results of tests and procedures are used to:

- do the research
- oversee the research
- see if the research was done correctly

Where is participant's personal information held?

Participant information is held in a research database housed at Radiation Therapy Oncology Group, RTOG and at the University of Pennsylvania (location of RadComp's Coordinating Center) in a Secure Portal. The RadComp Secure Portal was developed to capture sensitive personal information for subjects enrolled in the RadComp study. The portal is password protected and only authorized users of the study are allowed access. Users must adhere to

strict data security protocols set out by RadComp, HIPAA, and the IRB, when accessing the database to protect participant data. Within the portal, social security numbers are stored separately from other personally identifiable information, such as name and contact information, as an additional protection measure.

Neither RTOG nor the University of Pennsylvania may re-use or re-disclose information collected in this study for a purpose other than this study unless:

- You have given written authorization
- The Institutional Review Board has ensured appropriate privacy safeguards are in place

While RadComp study staff make every effort possible to ensure data protection, other groups and agencies such as Institutional Review Boards and Data Safety Monitoring Committees provide oversight of the trial to protect your rights and safety. These groups monitor clinical trials to ensure compliance with HIPAA (Health Insurance Portability and Accountability Act). Furthermore, healthcare networks maintain securities such as “fire walls,” or digital walls standing between protected health data and malware, to protect against security breaches by monitoring incoming and outgoing electronic traffic. Taken together, we hope this provides some peace of mind for the protection and security of your personal information.

For questions or concerns, feel free to contact us: radcomp@pennmedicine.upenn.edu or

215-662-6694